谈谈素数

TANTAN SUSHU

王 元

上海教育出版社

谈 谈 素 数

王　元

上海教育出版社

内 容 提 要

素数论这一古老的数学分支，包含着许多诸如哥德巴赫问题那样的有趣而又艰深的难题。为了解决这些问题，素数论既借助也带动了其他数学分支的发展，因而素数论迄今仍是一个活跃的领域。

本书旨在介绍素数论的主要内容，书中谈到了许多著名的数论问题和猜想，简介了解决这些问题的方法和近代成果，介绍了我国数学家在这个领域里的重要贡献。本书的前一半只用到了中学的数学知识，而具备一些数学分析的知识后就可以读完后一半。全书写法简洁，深入浅出，可供中学生和广大数学爱好者阅读。

谈 谈 素 数

王 元

上海教育出版社出版

（上海永福路 123 号）

新华书店上海发行所发行　江苏高邮印刷厂印刷

开本 787×1092　1/32　印张 2.5　字数 51,000

1978 年 11 月第 1 版　1983 年 4 月第 2 次印刷

印数 50,001—65,000 本

统一书号：7150·1947　　定价：0.20 元

目　录

序　言

在数学中,数论是研究数的性质,特别是研究整数性质的分支,它和几何学一样,是最古老的数学分支.

素数就是除 1 与其自身外，没有其他因数的大于 1 的自然数. 在自然数列中,最初的几个素数是

$$2, 3, 5, 7, 11, 13, 17, \cdots.$$

素数的性质是数论最早的研究课题之一，现在则已发展成为数论的一个独立分支——素数论. 素数论是数论中十分有味与引人入胜的一个分支，它里面有着许多没有解决的奇妙的猜测.

这本小册子将介绍素数论方面的一些结果，前面一部分(§1～§11)是算术部分. 在中学的数学课中，平面几何学是训练逻辑推导最好的课程. 此外，初等数论也能起到这个作用，它有助于培养分析问题和解决问题的能力. 这一部分并不涉及更多的定义与知识,所以只要耐心阅读,高中的同学是可以看得懂的. 但素数论方面的重要与深刻的结果，常常是用精深的数学方法，特别是精深的分析方法得到的. 如果不讲这一部分,就会给人以错觉，好象近代的素数论研究，只要从整数与素数的定义出发，作一些算术推导就行了. 事实当然不是这么回事,所以在 §12～§23 中,我们将假定读者学过微积分并了解实数的极限概念. 这一部分着重介绍近代素数论的一些问题与结果，而将证明省略了. 讲这一部分的目的是给读者增加一点数学常识. 属于近代数学的那些结论中,

能让非专业人员了解的，也许除数论以外就不多了．从这里也不难看到，虽然素数论中的许多问题表面上提法都很简单，但是近代素数论的重要成就，却往往是在近代数学成就的基础上，通过十分迂回的道路而得到的．反过来，为了解决素数论中的问题，也曾多次刺激并带动了其他不少数学分支的重要发展．因此素数论在数学中并不是孤立的，而是与很多数学分支密切相关的．由上所述，我们认为企图从整数与素数的定义出发，用简单的算术方法来处理这一类问题是不易收效的．不少事例表明这样做往往劳而无功，我们应该从中总结经验教训．总之，我们认为有兴趣于这类经典问题(例如哥德巴赫问题)的人，应该具备相当的数学知识与修养，而且应该先熟习素数论中已有的成果与方法，再作进一步的探讨，才可能会是有益的．

这本小册子取材于华罗庚老师的著作《数论导引》(科学出版社，1957 年)，《指数和的估计及其在数论中的应用》(科学出版社，1963 年)及夕尔宾斯基著《关于素数——我们已知和未知的》(波兰，华沙，1961 年)．笔者仅仅作了一些整理与归纳，使读者更便于了解素数论的概貌．另外，由于上面几本著作都已出版十多年了，所以本书也引征了一些新的文献，供作参考．

在撰写的过程中，承蒙陈景润同志的热情支持与帮助，又承蒙于坤瑞、徐广善等同志帮助准备手稿，他们提出了不少宝贵的意见．我谨在此向他们致以最衷心的感谢．限于笔者的水平，错误与不妥之处，还希望读者不吝指教．

王　元

1978 年 5 月于北京

§1. 素数与复合数

自然数是指

$$1, 2, 3, \cdots$$

中的数. 整数是指

$$\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots$$

中的数. 所以自然数就是正整数.

任意给出二整数 a 与 b, 其中 $b>0$. 如果有一个整数 c 使

$$a=bc,$$

就称 b 可以整除 a, a 称做 b 的倍数, b 称做 a 的因数. 记为 $b|a$. 假若 b 不能整除 a, 就记做 $b\nmid a$. 注意, 这里因数都是正的. 记

$$|a|=\begin{cases} a, & \text{当 } a\geqslant 0, \\ -a, & \text{当 } a<0. \end{cases}$$

我们称 $|a|$ 为 a 的绝对值. 如果 $b|a$, 而且 $1<b<|a|$, 我们就称 b 是 a 的真因数.

显然, 对于任何正整数 a 都有

$$1|a, \ a|0, \ a|a,$$

这说明 a 至少有因数 1 和 a.

自然数可以分成三类:

1) 1, 只有自然数 1 为它的因数.

2) p, 正好有而且只有自然数 1 及 p 为它的因数. 换句话说, p 是大于 1 而又没有真因数的自然数.

3) n, 有两个以上大于1的因数. 换句话说, n是有真因数的自然数.

第2)类数叫素数. 例如

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \cdots.$$

我们常常用 p, q, r, p_1, p_2, …等等来表示素数.

第3)类数叫复合数. 例如

$$4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, \cdots.$$

我们常常用 n, l, m, a, b, …等等来表示复合数.

2能整除的自然数叫做偶数, 如2, 4, 6, 8, …. 而2不能整除的自然数叫做奇数, 如1, 3, 5, 7, …. 显然大于2的偶数都是复合数. 所以只有一个偶素数2, 其余的素数都是奇素数.

§2. 唯一分解定理

引理1. 大于1的自然数 n 都可以分解成为素数的乘积.

证　如果 n 本身就是一个素数, 那末定理就已经成立了. 现在假定 n 是复合数, 那末 n 总有一个最小的真因数 q_1. 我们先证明 q_1 一定是素数. 如果 q_1 是复合数, 那末 q_1 还有真因数 r_1, 当然 $r_1 < q_1$, 而且 r_1 也是 n 的真因数. 这与 q_1 是 n 的最小真因数相矛盾, 所以 q_1 是素数. 记

$$n = q_1 n_1, \qquad 1 < n_1 < n.$$

如果 n_1 已经是素数, 那末定理即成立. 如果 n_1 不是素数, 假定 q_2 是 n_1 的最小素因数, 即得

$$n = q_1 q_2 n_2, \qquad 1 < n_2 < n_1 < n,$$

我们继续实行上面这种手续，得 $n>n_1>n_2>\cdots>1$. 所以这种手续不能超过 n 次. 最后得

$$n=q_1q_2\cdots q_k,$$

其中 $q_1, q_2, \cdots, q_k$ 都是素数（注意：q_1、q_2、$\cdots$、q_k 不一定是互不相同的）. 这个式子叫做 n 的素因数分解式. 引理证完.

例如：$$10,725=3^1\cdot5^2\cdot11^1\cdot13^1.$$

我们可以把大于 1 的自然数 n 的素因数分解式写成

$$n=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k},$$

其中 $p_1<p_2<\cdots<p_k$ 都是素数，而 $a_1, a_2, \cdots, a_k$ 都是自然数. 这个式子叫做 n 的标准分解式.

引理 2. 如果 p 是素数而且 $p|ab$，那末必定 $p|a$ 或 $p|b$.

证　不妨假定 a, b 都是自然数. 假定引理不成立，那末一定有一个最小的素数 p 使引理不成立. 对于这个素数 p，又有最小的 ab 使引理不成立，即 $p|ab$ 而 $p\nmid a$, $p\nmid b$.

我们先来证明 $a<p$, $b<p$. 假如不然，例如假定 $a>p$. 由于 $p\nmid a$，所以用 p 除 a，所得的余数 a_1 必在 0 与 p 之间，即

$$a=kp+a_1,\quad 0<a_1<p.$$

因此

$$ab=(kp+a_1)b=kbp+a_1b.$$

由 $p|ab$ 及 $p|kbp$ 得 $p|(ab-kbp)$，即 $p|a_1b$. 然而 $p\nmid a_1$, $p\nmid b$，从而有 $a_1b<ab$ 使引理不成立. 这与 ab 是使引理不成立的最小数的定义相矛盾. 所以 $a<p$，同理可知 $b<p$，因此 $ab<p^2$.

现在来证明 $p|ab$ 而 $p\nmid a$, $p\nmid b$ 将引出矛盾. 因 $p|ab$，所以 $ab=lp$. 若 $l=1$，那末 p 有真因数 a 与 b. 这与素数的定义相矛盾. 因此 $l>1$. 另一方面，上面已证 $ab<p^2$，所以 $l<p$.

由引理1的证明可知，假定 q 是 l 的最小非1的因数，那末 q 为素数．由于 $l|ab$，所以 $q|ab$．因为 $q\leqslant l<p$，所以由 p 是最小的使引理不成立的素数这一假定，可知 $q|a$ 或 $q|b$．我们不妨假定 $q|a$．记 $a=a'q$．由于前设 $q|l$．记 $l=tq$，代入 $ab=lp$ 得

$$a'qb=tqp.$$

因而 $a'b=tp$，即 $p|a'b$．但这样 $a'b<ab$，$p\nmid a'$，$p\nmid b$．这与关于 p 与 ab 的假定相矛盾．引理证完．

定理1(唯一分解定理)．大于1的自然数 n 的标准分解式是唯一的．换句话说，如果不计次序，那末 n 只有唯一的方法表示成素数的乘积．

证　由引理2显然可知，如果 p 是素数，

$$p|ab\cdots c,$$

那末 p 一定能整除 a，b，…，c 中的一个．又如果 a，b，…，c 都是素数，那末 p 一定是 a，b，…，c 中的一个．

假定 n 有两种标准分解式

$$n=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}=q_1^{b_1}q_2^{b_2}\cdots q_l^{b_l}.$$

那末任何 p_i 必定为 q_1，q_2，…，q_l 中的一个，任何 q_j 也必定为 p_1，p_2，…，p_k 中的一个．所以 $k=l$．由于

$$p_1<p_2<\cdots<p_k \quad 及 \quad q_1<q_2<\cdots<q_k,$$

所以

$$p_i=q_i, \qquad 1\leqslant i\leqslant k.$$

最后，如果有 $a_i>b_i$，这儿 $1\leqslant i\leqslant k$，那末以 $p_i^{b_i}$ 除 n 的标准分解式得

$$p_1^{a_1}\cdots p_i^{a_i-b_i}\cdots p_k^{a_k}=p_1^{b_1}\cdots p_{i-1}^{b_{i-1}}p_{i+1}^{b_{i+1}}\cdots p_k^{b_k}.$$

上式的左边是 p_i 的倍数，但右边不是，这不可能．同样 $a_i<b_i$ 也是不可能的，所以

$$a_i=b_i,\qquad 1\leqslant i\leqslant k.$$

定理证完.

顺便说一句,我们不把1看成素数,是因为如果把1看成素数,那末在n的标准分解式前面,可以乘上1的任何次幂,这就破坏了标准分解式的唯一性了.

虽然在理论上,任何自然数n都是可以写成标准分解式的. 但当n很大时,具体写出n的标准分解式来却是很不容易的事. 有时甚至连n的一个素因数也找不出来. 例如人们已经证明$M_{101}=2^{101}-1$(共31位)是两个不同素数的乘积,其中较小的一个至少有11位,但我们至今还不知道这两个素因数是什么[1]. 又例如在1958年,人们就知道$F_{1945}=2^{2^{1945}}+1$的最小素因数$p=5\times 2^{1947}+1$. 但至今我们并不知道F_{1945}的其他素因数[2]. 由于

$$2^{1945}=32\times 2^{1940}=32\times(2^{10})^{194}>30\times(10^3)^{194}$$
$$=3\times 10^{583},$$

所以

$$F_{1945}>2^{3\times 10^{583}}=(2^{10})^{3\times 10^{582}}>10^{9\times 10^{582}},$$

即F_{1945}是一个超过10^{582}位的自然数,而p则是一个有587位的素数.

假定a与b是两个整数,但不都是0. 如果$c|a$, $c|b$, 我们就称c是a与b的公因数. 如果$a\neq 0$, 那末由$c|a$可得$a=cd$, 其中$d\neq 0$是整数,即$|d|\geqslant 1$. 所以,$|a|=|cd|=c|d|\geqslant c$,即a与b的公因数c不大于a的绝对值$|a|$. 因此,a与

---

[1] J. Brillhart and G. D. Johnson, On the factors of certain Mersenne numbers, *Math. Comp.*; **14** (1960), 553～555.

[2] R. M. Robinson, A report on primes and on factors of Fermat numbers, PAMS; **9** (1958), 673～681.

b 的公因数中一定有一个最大的，称为 a 与 b 的**最大公因数**，记为(a, b). 例如

$$(5, 3)=1, \qquad (20, 45)=5,$$
$$(11, -242)=11, \qquad (0, -377)=377$$

等等. 如果$(a, b)=1$, 就称 a 与 b **互素**.

我们用 $r=\min(m, n)$表示 r 等于 m 与 n 中较小的一个. 例如 $5=\min(5, 13)$. 我们又用 $s=\max(m, n)$表示 s 等于 m 与 n 中较大的一个. 例如 $13=\max(5, 13)$.

定理 2. 假定 a 与 b 是二正整数，把它们写做

$$a=p_1^{a_1}\cdots p_s^{a_s}, \qquad a_1\geqslant 0, \cdots, a_s\geqslant 0,$$
$$b=p_1^{b_1}\cdots p_s^{b_s}, \qquad b_1\geqslant 0, \cdots, b_s\geqslant 0,$$

其中 $p_1<\cdots<p_s$ 都是素数. 那末

$$(a, b)=p_1^{c_1}\cdots p_s^{c_s},$$

其中 $c_i=\min(a_i, b_i)\ (1\leqslant i\leqslant s)$.

证　如果 $c|a$, $c|b$, 那末由引理 2 可知 c 的素因数只能是 $p_1, \cdots, p_s$, 即

$$c=p_1^{d_1}\cdots p_s^{d_s}.$$

显然 $d_1\leqslant a_1$, $d_1\leqslant b_1$, 所以, $d_1\leqslant\min(a_1, b_1)=c_1$. 同理 $d_i\leqslant c_i\ (2\leqslant i\leqslant s)$. 因此

$$c\leqslant p_1^{c_1}\cdots p_s^{c_s}.$$

即 a、b 的任何公因数 c 不大于 $p_1^{c_1}\cdots p_s^{c_s}$. 另一方面，$p_1^{c_1}\cdots p_s^{c_s}|a$, $p_1^{c_1}\cdots p_s^{c_s}|b$, 即 $p_1^{c_1}\cdots p_s^{c_s}$ 是 a、b 的公因数. 所以 $p_1^{c_1}\cdots p_s^{c_s}$ 是 a 与 b 的最大公因数. 定理证完.

§3. 素数有无穷多

现在发生一个问题，素数究竟只有有限多个呢？还是有

无穷多？这件事早在欧几里德(Euclid)就已经知道了：素数有无穷多.

定理 1. 素数有无穷多.

证　如果素数的个数有限，那末我们就可以将全体素数列举如下：

$$p_1,\ p_2,\ \cdots,\ p_k.$$

命

$$q=p_1p_2\cdots p_k-1.$$

q 总是有素因数的. 但我们可证明任何一个 $p_i(1\leqslant i\leqslant k)$ 都除不尽 q：假若不然，由 $p_i|q$ 及 $p_i|p_1p_2\cdots p_k$ 就得到 $p_i|(p_1p_2\cdots p_k-q)$，即 $p_i|1$，这是不可能的. 故任何一个 p_i 都除不尽 q，这说明 q 有不同于 $p_1,\ p_2,\ \cdots,\ p_k$ 的素因数. 这与 $p_1,\ p_2,\ \cdots,\ p_k$ 是全体素数的假定相矛盾，所以素数有无穷多. 定理证完.

由定理 1 的证明立刻可以推出：

定理 2. 假定 $n>2$，那末在 n 与 $n!$ ($n!$ 表示不超过 n 的自然数的连乘积，即 $n!=1\cdot2\cdot\cdots\cdot n$)之间一定有一个素数.

证　假定不超过 n 的素数为 $p_1,\ p_2,\ \cdots,\ p_k$. 又假定 $q=p_1p_2\cdots p_k-1$. 由于 $n>2$，所以 $q>4$. 由定理 1 的证明可知 q 有一个不同于 $p_1,\ p_2,\ \cdots,\ p_k$ 的素因数 p，所以 $p>n$. 另一方面，$p\leqslant q\leqslant n!-1<n!$. 定理证完.

定理 1 的证明方法还可以用来证明更广泛的结果. 例如：

定理 3. 形如 $4n+3$ 的素数有无穷多.

证　如果形如 $4n+3$ 的素数有限，则可假定它们的全体是

$$p_1,\ p_2,\ \cdots,\ p_k.$$

命

$$q=4p_1p_2\cdots p_k-1=4(p_1p_2\cdots p_k-1)+3.$$

从而 q 是形如 $4n+3$ 的，而且任何 $p_i\,(1\leqslant i\leqslant k)$ 都除不尽 q. 由于除掉 2 以外，素数都是奇数，因此奇素数用 4 除以后，所得的余数必定是 1 或 3. 又由于两个 4 除余 1 的数 $4l+1$ 与 $4m+1$ 相乘得

$$(4l+1)(4m+1)=4(4lm+l+m)+1,$$

仍然是一个 $4n+1$ 型的数. 因 q 是 $4n+3$ 型的数，所以 q 的素因数不可能都是形如 $4n+1$ 的数，即 q 还有形如 $4n+3$ 的素因数，但又不能是 $p_1, p_2, \cdots, p_k$ 中的一个. 这与对于 $p_1, p_2, \cdots, p_k$ 的假定相矛盾. 所以形如 $4n+3$ 的素数有无穷多. 定理证完.

读者可以仿照以上证法，证明形如 $6n+5$ 的素数有无穷多. 形如 $4n+1$ 的素数也有无穷多，这将在 §8 中证明.

虽然素数的个数有无穷多，但我们并不能写出任意大的素数来. 目前所知道的最大素数都是通过特殊的方法，而且借助于电子计算机才得到的. 现在我们知道的最大素数是

$$M_{19937}=2^{19937}-1,$$

共 6002 位[1].

§4. 素 数 表

所谓素数表，就是造一张表，其中包括不超过已知自然数 N 的所有素数. 先讲一条引理.

---

[1] B. Tuckerman, The 24-th Mersenne Prime, PNAS USA, 1971, 2319～2320.

引理 1. 每一个复合数 n 至少有一个素因数 $\leqslant\sqrt{n}$.

证　假定 p 是 n 的最小真因数，那末由引理 2.1(即 §2，引理 1)的证明可知 p 是素数．现在来证明 $p\leqslant\sqrt{n}$．由于 n 是复合数，所以可以将 n 写作 $n=pn_1$．因 p 是 n 的最小因数，所以 $n_1\geqslant p$．如果 $p>\sqrt{n}$，就有 $n=pn_1>\sqrt{n}\cdot\sqrt{n}=n$．矛盾．所以 $p\leqslant\sqrt{n}$．引理证完．

我们先找出不超过 $\sqrt{N}$ 的全部素数，依次排列如下：

$$2=p_1<p_2<\cdots<p_r\leqslant\sqrt{N}.$$

然后把大于 1，而又不超过 N 的自然数，按大小次序排列如下：

$$2,\ 3,\ \cdots,\ N.$$

在其中留下 $p_1=2$，而把 p_1 的倍数全部划掉，再留下 p_2，而把 p_2 的倍数都划掉，继续这一手续，最后，留下 p_r，而把 p_r 的倍数都划掉．留下的就是不超过 N 的全体素数了．这是因为由引理 1 可知，如果 $n\leqslant N$ 而又是复合数，那末 n 必定有一个素因数 $\leqslant\sqrt{N}$，所以被划掉了．如果 n 是 $\leqslant\sqrt{N}$ 的素数，那末规定 n 留下．如果 n 是满足 $\sqrt{N}<n\leqslant N$ 的素数，那末 n 不会是任何 $p_i(1\leqslant i\leqslant r)$ 的倍数，所以 n 也留下来了．因此留下来的是不超过 N 的全体素数．

例如要求出不超过 50 的全体素数，因为不超过 $\sqrt{50}<8$ 的素数是 2, 3, 5, 7, 所以在 2, 3, …, 50 中，留下 2, 3, 5, 7, 依次划去 2, 3, 5, 7 的倍数

2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~,
11, ~~12~~, 13, ~~14~~, ~~15~~, ~~16~~, 17, ~~18~~, 19, ~~20~~,
~~21~~, ~~22~~, 23, ~~24~~, ~~25~~, ~~26~~, ~~27~~, ~~28~~, 29, ~~30~~,
31, ~~32~~, ~~33~~, ~~34~~, ~~35~~, ~~36~~, 37, ~~38~~, ~~39~~, ~~40~~,
41, ~~42~~, 43, ~~44~~, ~~45~~, ~~46~~, 47, ~~48~~, ~~49~~, ~~50~~.

留下的数

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,$$
$$23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47.$$

就是不超过 50 的全体素数.

上面讲的就是著名的埃拉多斯染尼氏 (Eratosthenés) 筛法. 早在公元前三百年左右, 埃氏就提出这一方法. 素数表都是根据这一方法略加变化而造出来的. 埃氏筛法的改进与发展,是近代解析数论的重要工具之一.

1909 年, 莱茉[1]发表了不超过 10^7 的素数表. 在表中凡 $\leqslant$10, 170, 600, 而又不能被 2, 3, 5, 7 整除的自然数, 它的最小素因数都被列了出来. 还有居立刻 (J. F. Kulik, 1793～1863), 他曾造出不超过 10^8 的素数表, 他的手稿存放于维也纳科学院内. 1951 年, 居立刻(J. P. Kulik), 波来梯与波尔特[2]曾发表了不超过 1.1×10^7 的素数表, 即在莱茉氏表的基础上增加了由 10,006,741 至 10,999,997 之间的所有素数. 他们在造表过程中,用了居立刻(J. F, Kulik)的手稿.

自从有了电子计算机后, 更大得多的素数表被制作出来了. 1959 年, 贝克尔与格伦贝尔格[3]制成含有不超过 $p_{6,000,000}=104,395,301$ 的全体素数 (共 6×10^6 个素数) 的微型卡片. 六十年代初, 美国学者就曾宣称, 他们将在电子计算机的存储系统中存放前 5×10^8 个素数.

---

[1] D. N. Lehmer, Factor table for the first ten millions, Washington, Carnegie Institute, 1909.

[2] J. P. Kulik, L, Poletti and R. J. Porter, Liste des nombres premiers du onzième million (plus précisément de 10, 006, 741 à 10, 999, 997), Amsterdam, 1951.

[3] C. L. Backer and F. L. Gruenberger, The first six million prime numbers. The RAND Corp. Santa Monica, Pub. Microcard Foun; Madison, Wisconsin, 1959.

§5. 费　马　数

定理 1. 如果 2^m+1 是素数，那末 $m=2^n$.

证　如果 m 有一个奇数真因数 q，那末 $m=qr$，且

$$2^m+1=2^{qr}+1=(2^r)^q+1$$
$$=(2^r+1)(2^{r(q-1)}-\cdots-2^r+1).$$

因为 $1<2^r+1<2^m+1$，所以 2^m+1 有真因数 2^r+1，即不是素数. 矛盾. 因此 m 不能有奇数真因数，即 $m=2^n$. 定理证完.

形状是 $F_n=2^{2^n}+1$ 的数叫做费马(P. Fermat)数. 当 $n=0, 1, 2, 3, 4$ 时，

$$F_0=3,\ F_1=5,\ F_2=17,\ F_3=257,\ F_4=65,537.$$

都是素数. 由此，费马曾猜测，所有的费马数都是素数，即定理 1 的逆也是成立的. 但是在 1732 年，欧拉(L. Euler)证明了：

$$F_5=2^{2^5}+1=641\times 6,700,417.$$

这可以证明如下：记 $a=2^7$，$b=5$，那末 $a-b^3=3$，$1+ab-b^4=1+(a-b^3)b=1+3b=2^4$，所以 $F_5=2^{2^5}+1=(2a)^4+1=2^4\cdot a^4+1=(1+ab-b^4)a^4+1=(1+ab)a^4+1-a^4b^4=(1+ab)(a^4+(1-ab)(1+a^2b^2))$，即 $(1+ab)\mid F_5$，而 $1+ab=641$. 从而费马猜想被否定了.

到今天为止，我们只知道上面 5 个费马数是素数. 此外，我们已证明了 46 个费马数是复合数. 这些复合数可以分成三类[1]：

[1] J. C. Hallyburton, Jr. and J. Brillhart, Two new factors of Fermat numbers, *Math. Comp.*; **1** (1975), 109～112.

1) 当 $n=5, 6, 7$ 时，我们知道 F_n 的标准分解式.

2) 当 $n=9, 10, 11, 12, 13, 15, 16, 18, 19, 21, 23, 25, 26, 27, 30, 32, 36, 38, 39, 42, 52, 55, 58, 63, 73, 77, 81, 117, 125, 144, 150, 207, 226, 228, 250, 267, 268, 284, 316, 452, 1945$ 时，我们只知道 F_n 的部分素因数，但并不知道它们的全部素因数.

3) 当 $n=8, 14$ 时，我们只知道 F_n 是复合数，但它的任何真因数我们都不知道.

当 $n=17, 20, 22, 24, \cdots$ 时，我们还不知道 F_n 是素数还是复合数.

因此在费马数中，是否有无穷多个素数？或者是否有无穷多个复合数？都是没有解决的问题.

高斯(C. F. Gauss)曾经证明过，如果 F_n 是素数，那末正 F_n 边形是可以用圆规与直尺来作图的. 这说明费马数与平面几何学的一些问题有着深刻的内在联系.

费马数有一个有趣的性质，即当 $k>0$ 时有 $(F_n, F_{n+k})=1$. 事实上，设自然数 $m|F_n$ 及 $m|F_{n+k}$. 命 $a=2^{2^n}$. 则利用首项为 -1，公比为 $-a$ 的几何级数的求和公式得

$$\frac{F_{n+k}-2}{F_n}=\frac{2^{2^{n+k}}-1}{2^{2^n}+1}=\frac{a^{2^k}-1}{a+1}$$

$$=a^{2^k-1}-a^{2^k-2}+\cdots+a-1,$$

所以 $F_n|(F_{n+k}-2)$. 因 $m|F_n$，因此 $m|(F_{n+k}-2)$. 再由 $m|F_{n+k}$，即得 $m|2$. 但费马数都是奇数，所以必定有 $m=1$. 于是证明了 $(F_n, F_{n+k})=1$. 由此推出，在数列

$$F_0, F_1, F_2, \cdots$$

中，每个数的素因数都两两不同. 这就再次得出素数有无穷多(即定理 3.1). 由此也推出了第 $n+2$ 个素数 p_{n+2} 适合于

$$p_{n+2} \leqslant F_n = 2^{2^n} + 1.$$

设 F_n 的最大素因数为 $p(F_n)$. 用数论中深刻的丢番图逼近论方法，斯梯瓦特[1]证明了存在常数 $A>0$ 使

$$p(F_n) > An2^n, \quad n=1, 2, \cdots$$

§6. 麦什涅数

定理 1. 如果 $n>1$, 且 a^n-1 是素数，那末 $a=2$, 且 n 是素数.

证　如果 $a>2$, 又因 $n>1$, 所以 $1<a-1<a^n-1$, 且 $a^n-1=(a-1)(a^{n-1}+a^{n-2}+\cdots+a+1)$, 所以 a^n-1 有真因数 $(a-1)$, 即它不是素数了. 因此 $a=2$. 如果 n 是复合数，即 $n=kl$, 其中 $1<k<n$, 那末 $1<2^k-1<2^n-1$, 且 $(2^k-1)\mid(2^n-1)$. 从而 2^n-1 也将不是素数了. 所以如果 a^n-1 是素数，则必须 $a=2$ 及 n 是素数. 定理证完.

形状是 $M_n=2^n-1$ 的数叫麦什涅 (M. Mersenne) 数. 由定理 1 可知，如果 M_n 是素数，则必须 n 是素数. 但反过来并不对：当 n 是素数时，M_n 不一定是素数. 例如

$$23\mid M_{11}, \ 47\mid M_{23}, \ 167\mid M_{83}, \ 263\mid M_{131}, \ 359\mid M_{179}$$

等等.

到今天为止，我们只知道 24 个麦什涅数是素数. 它们是 M_p, 其中 $p=2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937$. 从第 13 个开始，即从 M_{521} 开始，都是在 1952

[1] C. L. Stewart, On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, PLMS(将发表).

年以后，借助于电子计算机而陆续发现的．§3中已经提到过的目前所知道的最大素数，就是麦什涅素数 M_{19937}.

麦什涅数中是否有无穷多个素数？是一个没有解决的问题．

还有人提出过这样的猜想，即如果 M_p 是素数，那末 M_{M_p} 也是一个素数．

这个猜想对于小的麦什涅素数都是对的．但到第5个麦什涅素数 $M_{13}=8191$，这个猜想就被否定了．借助于电子计算机，可以证明 $M_{M_{13}}=2^{8191}-1$ 是一个复合数．这个数有2466位，但我们还不知道它的任何素因数[1]．到1957年，有人证明了虽然 M_{17} 与 M_{19} 都是素数，但 $M_{M_{17}}$ 与 $M_{M_{19}}$ 都是复合数，它们可以分别被 $1768(2^{17}-1)+1$ 与 $120(2^{19}-1)+1$ 整除[2]．

与麦什涅数密切相关的是寻找偶完全数的问题．所谓完全数 n，是指 n 的全部因数之和等于 $2n$ 的数．例如6，它的因数之和是 $1+2+3+6=12$．又如28，它的因数之和是 $1+2+4+7+14+28=56$．所以6与28都是偶完全数．

定理2．如果 M_p 是素数，那末

$$\frac{1}{2}M_p(M_p+1)=2^{p-1}(2^p-1)$$

是一个偶完全数，而且除了这些以外，再没有其他的偶完全数．

证　我们用 $\sigma(n)$ 表示 n 的全部因数之和．如果 M_p 是素

---

[1] R. M. Robinson, Mersenne and Fermat numbers, PAMS; **5** (1954), 842～846.

[2] R. M. Robinson, Some factorizations of numbers of the form $2^n\pm1$, MTAC; **11** (1957), 265～268.

数，那末$\frac{1}{2}M_p(M_p+1)=2^{p-1}M_p=2^{p-1}(2^p-1)$的因数显然为$1, 2, 2^2, \cdots, 2^{p-1}, M_p, 2M_p, \cdots, 2^{p-1}M_p$，所以

$$\begin{aligned}\sigma(2^{p-1}(2^p-1))&=1+2+\cdots+2^{p-1}\\&\quad+(2^p-1)(1+2+\cdots+2^{p-1})\\&=(1+2+\cdots+2^{p-1})(1+2^p-1)\\&=2^p(2^p-1)=2\cdot 2^{p-1}(2^p-1).\end{aligned}$$

即$\frac{1}{2}M_p(M_p+1)=2^{p-1}(2^p-1)$是一个偶完全数．

现在假定a是一个偶完全数．假设a的标准分解式中含2的最高方幂的次数为$n-1$．因a为偶数，所以$n-1\geqslant 1$．又因2^{n-1}显然不是偶完全数，所以

$$a=2^{n-1}u,\ u>1,\ 2\nmid u.$$

因此a的因数为所有形如$2^i v$的数，其中$0\leqslant i\leqslant n-1$及$v|u$．从而

$$\begin{aligned}2^n u=2a=\sigma(a)&=(1+2+\cdots+2^{n-1})\sigma(u)\\&=\sigma(u)(2^n-1).\end{aligned}$$

即得$(2^n-1)|2^n u$．因$(2^n,\ 2^n-1)=1$，所以$(2^n-1)|u$，即$\frac{u}{2^n-1}$是整数．另一方面，由上面的等式得到

$$\sigma(u)=\frac{2^n u}{2^n-1}=u+\frac{u}{2^n-1}.$$

但u与$\frac{u}{2^n-1}$都是u的因数，而$\sigma(u)$又是u的所有因数的总和，所以u只有两个因数u和$\frac{u}{2^n-1}$．因$u>1$及u至少有两个因数u与1，所以必须$\frac{u}{2^n-1}=1$．换句话说，u是一个素数，且

$$u=2^n-1.$$

由定理 1，n 必须是素数．这就证明了 $a=2^{n-1}(2^n-1)=\frac{1}{2}M_n(M_n+1)$，$n$ 是素数．定理证完．

这个定理说明，是否有无穷多个偶完全数的问题，即归结为是否有无穷多个麦什涅素数的问题．由于目前共知道 24 个麦什涅素数，所以目前只知道 24 个偶完全数，其中最大的是

$$2^{19936}(2^{19937}-1).$$

但是是否存在奇完全数呢？这是一个没有解决的问题．借助于电子计算机可以证明，如果 n 是奇完全数，那末 $n>10^{50}$，又如果 n 是奇完全数，那末它一定有一个大于 100,110 的素因数[1,2]．

§7. 特殊数列中的素数

所谓斐波那契(L. Fibonacci)数列就是由递推公式

$$u_1=u_2=1,\ u_{n+2}=u_{n+1}+u_n(n=1,\ 2,\ \cdots)$$

定义的正整数数列．例如：$u_1=1$，$u_2=1$，$u_3=2$，$u_4=3$，$u_5=5$，$u_6=8$，$u_7=13$，$u_8=21$，$\cdots$．

我们已经知道，当 $n=3, 4, 5, 7, 11, 13, 17, 23, 29, 43, 47$ 时，u_n 是素数，其中

$$u_{47}=2,971,215,073.$$

除这 11 个素数外，我们还不知道别的 u_n 是素数，更不知道在

[1] P. Hagis, Jr; A lower bound for the set of odd perfect numbers, *Math. Comp.*; **27**: 124 (1973), 951～953.

[2] P. Hagis, Jr; and W. L. McDaniel, On the largest prime divisor of an odd perfect numbers, II, *Math. Comp.*; **29** (1975), 922～924.

数列 $u_n(n=1, 2, \cdots)$ 中是否有无穷多个素数.

数列 $v_n(n=1, 2, \cdots)$ 的定义如下:

$$v_1=1,\ v_2=3,\ v_{n+2}=v_{n+1}+v_n(n=1, 2, \cdots).$$

这也叫做斐波那契数列. v_n 与 u_n 的差别仅在于初始值取得不同, 即 $n=1, 2$ 时, 所取的值不同, 以后的值都是由同样的递推公式 $u_{n+2}=u_{n+1}+u_n$ 得到的. 例如 $v_1=1$, $v_2=3$, $v_3=4$, $v_4=7$, $v_5=11$, $u_6=18$, $v_7=29$, $\cdots$.

当 $n=2, 4, 5, 7, 8, 11, 13, 17, 19, 31, 37, 41, 47, 53, 61, 71$ 时, v_n 是素数, 其中

$$v_{71}=688,846,502,588,399.$$

除这 16 个素数外, 我们还不知道别的 v_n 是素数. 更不知道在数列 $v_n(n=1, 2, \cdots)$ 中是否有无穷多个素数.

对于 u_n 和 v_n 的最大素因数 $p(u_n)$ 和 $p(v_n)$, 斯梯瓦特(见13页, 注[1])证明了存在正常数 A_1 和 A_2 使

$$p(u_n)\geqslant A_1\frac{n\log n}{q(n)^{4/3}},$$

$$p(v_n)\geqslant A_2\frac{n\log n}{q(n)^{4/3}},$$

$$n=3, 4, \cdots,$$

此处 $q(n)$ 表示 n 的无平方因数的因数个数.

又如在数列

$$1, 11, 111, 1111, \cdots$$

中是否有无穷多个素数呢?这问题也没有解决. 我们只知道很少几个这样形状的数是素数, 例如 11 与

$$11,111,111,111,111,111,111,111=\frac{10^{23}-1}{9}\text{[1]}.$$

---

[1] M. Kraïtchik, Recherches sur la théorie des nombres, 2 vols, paris, 1924～1929.

§8. 费马小定理

假定 m 为正整数．将整数 a 表为

$$a=qm+r,$$

此处 $0\leqslant r<m$，我们称 r 为 m 除 a 后所得的余数（注意：a 可以是负的）．在讲费马小定理以前，为了简便起见，我们先引进同余式的概念．如果整数 a 与 b 的差 $a-b$ 是 m 的倍数，就称 a 与 b 对模 m 同余．记为

$$a\equiv b\pmod m.$$

实际上，a 与 b 对模 m 同余的意思，就是用 m 除 a，b 以后，所得的余数相同．如果 a 与 b 对模 m 不同余，就记为

$$a\not\equiv b\pmod m.$$

例如　$31\equiv-9\pmod{10}$，$29\not\equiv 7\pmod 8$．

定理 1（费马）．如果 p 是素数，那末对于任何整数 a 都有

$$a^p\equiv a\pmod p.$$

证　假定 $p|a$，那末 $p|a^p$，所以 $p|(a^p-a)$．即定理成立．今后我们假定 $p\nmid a$．

显然如果 $p\nmid n$，那末 n 一定模 p 同余于

$$1,\ 2,\ \cdots,\ p-1 \tag{1}$$

中的一个，这是因为用 p 除 n 后的余数总是其中之一．假定在这 $p-1$ 个数中任取两个不同的数 k_1 与 k_2，现在来证明

$$k_1a\not\equiv k_2a\pmod p. \tag{2}$$

假若(2)不成立，即 $p|(k_1a-k_2a)=(k_1-k_2)a$，那末由引理 2.2 得 $p|(k_1-k_2)$ 或 $p|a$．由假定 $p\nmid a$，所以 $p|(k_1-k_2)$．又

由于$1\leqslant k_1\leqslant p-1$, $1\leqslant k_2\leqslant p-1$及$k_1\neq k_2$,所以$p\nmid(k_1-k_2)$. 得一矛盾,所以(2)式成立. 另一方面,如果$k$是(1)中的一个数,那末$p\nmid ka$, 因此$p-1$个数.

$$a,\ 2a,\ \cdots,\ (p-1)a \tag{3}$$

模p分别同余于(1)中的一个数, 而且(3)中的数又彼此对模p互不同余. 又因从$c\equiv d(\bmod p)$与$c'\equiv d'(\bmod p)$可以推出$cc'\equiv dd'(\bmod p)$,所以(1)中各数相乘的积模p同余于(3)中各数相乘的积,因此

$$a\cdot(2a)\cdot\cdots\cdot(p-1)a\equiv 1\cdot 2\cdot\cdots\cdot(p-1)(\bmod p),$$

$$(p-1)!a^{p-1}\equiv(p-1)!(\bmod p),$$

即$p\mid(p-1)!(a^{p-1}-1)$. 因为p是素数及引理2.2, 所以$p\nmid(p-1)!$. 再用引理2.2得$p\mid(a^{p-1}-1)$, 即得

$$a^p\equiv a(\bmod p).$$

定理证完.

每个奇数或者是形状$4n+1$,或者是形状$4n+3$. 我们已经知道形状是$4n+3$的素数有无穷多(见定理3.3). 现在我们来证明形状是$4n+1$的素数也有无穷多.

定理 2. 形状是$4n+1$的素数有无穷多.

证 假定m是一个大于1的整数,那末$m!$有因数2, 所以$m!$是偶数. 因为$m!^2+1$是一个大于1的奇数,所以它必定有一个奇素因数p. 现在证明p必定是形状$4k+1$的素数. 假定$p=4k+3$. 因为

$$\begin{aligned}m!^{p-1}+1&=m!^{2(2k+1)}+1\\&=(m!^2+1)(m!^{2\cdot 2k}-m!^{2\cdot(2k-1)}\\&\quad+\cdots-m!^2+1),\end{aligned}$$

所以

$$(m!^2+1)\mid(m!^{p-1}+1).$$

因此由 $p|(m!^2+1)$ 可得

$$p|(m!^p+m!).$$

由定理 1 可得

$$p|(m!^p-m!).$$

从而

$$p|(m!^p+m!-m!^p+m!).$$

即得

$$p|2\cdot m!.$$

因 p 是奇素数, 所以 $p\nmid 2$. 因此由引理 2.2 可知 $p|m!$. 从而 $p|m!^2$. 因为 $p|(m!^2+1)$, 所以 $p|1$, 矛盾. 因此对于每个自然数 $m>1$, $m!^2+1$ 的素因数 p 都是形如 $4k+1$ 的. 现在证明 $p>m$. 不然的话, 如果 $p\leqslant m$, 那末 $p|m!$, 所以 $p|m!^2$, 因而 $p|(m!^2+1-m!^2)$, 即 $p|1$. 矛盾. 所以 $p>m$. 由于 m 可以任意大, 所以形状是 $4k+1$ 的素数有无穷多. 定理证完.

由定理 1 可知, 如果 p 是奇素数, 那末

$$2^{p-1}\equiv 1(\bmod p).$$

但是否存在素数 p 使

$$2^{p-1}\equiv 1(\bmod p^2) \tag{4}$$

呢? 我们仅仅知道两个这样的素数, 即 1,093 与 3,511, 而且当 $p<100,000$ 时, 不再有素数 p 适合于(4)式. 至于使(4)式成立的素数是仅有有限多个呢? 还是无穷多个? 使(4)式不成立的素数仅有有限多个呢? 还是无穷多个? 我们都不知道.

由定理 1 可知, 如果 p 是素数, 那末

$$p|(1^{p-1}+2^{p-1}+\cdots+(p-1)^{p-1}+1). \tag{5}$$

1950 年, 居加(G. Giuga)猜测, 只有当 p 是素数时, (5)式才能

成立．这一猜想对于不超过$10^{1,000}$的整数都是对的．但我们还不能够加以证明．

§9. 拉格朗日定理与威尔逊定理

定理1(拉格朗日)．假定p是素数，那末同余方程

$$(1)\qquad f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\equiv0(\bmod p),\quad 1\leqslant x\leqslant p$$

的解数$\leqslant n$，重解也计算在内．这里a_n，a_{n-1}，…，a_0都是整数且$p\nmid a_n$.

证 如果(1)没有解，那末定理已经成立．如果$x=a$是(1)的一个解，那末(1)式可以写成

$$f(x)=(x-a)f_1(x)+r_1,$$

以$x=a$代入得$p|r_1$，所以

$$f(x)\equiv(x-a)f_1(x)(\bmod p).$$

如果$x=a$又是$f_1(x)\equiv0(\bmod p)$的解，那末同样可得

$$f_1(x)\equiv(x-a)f_2(x)(\bmod p).$$

这时我们称a做$f(x)\equiv0(\bmod p)$的重解．继续下去，如果

$$f(x)\equiv(x-a)^hg_1(x)(\bmod p),$$

其中$g_1(a)\not\equiv0(\bmod p)$，就称$a$是$f(x)\equiv0(\bmod p)$的$h$重解．由证明可以看出$g_1(x)$的次数是$n-h$.

设(1)另有一解$x=b$，那末

$$0\equiv f(b)\equiv(b-a)^hg_1(b)(\bmod p),$$

因$p\nmid(b-a)$，所以由引理2.2可知

$$g_1(b)\equiv0(\bmod p).$$

如果$x=b$是$g_1(x)\equiv0(\bmod p)$的k重解，那末同样有

$$f(x)\equiv(x-a)^h(x-b)^k g_2(x)\,(\bmod p).$$

这样继续进行下去可得

$$f(x)\equiv(x-a)^h(x-b)^k\cdots(x-c)^l g(x)\,(\bmod p).$$

其中 $g(x)$ 的次数是 $n-h-k-\cdots-l$，且 $g(x)\equiv 0(\bmod p)$ 不再有解，所以 $f(x)\equiv 0(\bmod p)$ 的解数是 $n-h-k-\cdots-l\leqslant n$ 定理证完.

由拉格朗日(J. L. Lagrange)定理立即推出下面的威尔逊(J. Wilson)定理.

定理 2(威尔逊). 如果 p 是素数，那末

$$(p-1)!\equiv -1(\bmod p). \tag{2}$$

证　由定理 8.1 可知同余方程

$$x^{p-1}-1\equiv 0(\bmod p),\quad 1\leqslant x\leqslant p$$

有 $p-1$ 个解 $1, 2, \cdots, p-1$，所以由定理 1 的证明可知

$$x^{p-1}-1\equiv(x-1)(x-2)\cdots(x-(p-1))\,(\bmod p).$$

以 $x=0$ 代入即得

$$-1\equiv(-1)^{p-1}(p-1)!\,(\bmod p).$$

当 $p=2$ 时定理显然成立. 当 $p>2$ 时，$2\mid(p-1)$，所以 $(-1)^{p-1}=1$，由上式即得(2)式. 定理证完.

定理 3. 大于 1 的自然数 n 为素数的充要条件是

$$(n-1)!\equiv -1(\bmod n). \tag{3}$$

证　由定理 2 可知，如果 $n=p$ 是素数，那末(3)式成立. 现在来证明，如果(3)式成立，那末 n 必定是素数. 实际上，假定 n 是复合数，即 $n=ab$，此处 $n>a>1$，那末 $a\mid(n-1)!$. 由(3)式可知 $a\mid((n-1)!+1)$，即推出 $a\mid 1$. 这是不可能的，所以 n 是素数. 定理证完.

条件(3)虽然是判别一个自然数 n 是否素数的充要条件. 但这一判别条件并没有什么应用价值. 例如当 n 是一个 3 位

数时，$(n-1)!+1$ 就是一个超过 100 位的数，所以计算量是非常大的.

由定理 2 出发，也可以提出这样的问题：是否有素数 p 使

$$(p-1)!+1\equiv 0 \pmod{p^2} \tag{3}$$

成立？当 $p\leqslant 30,000$ 时，只有 5, 13, 563 这三个素数满足(3)式[1]. 但我们还不知道适合于(3)式的素数是否有无穷多？

当 p 是大于 3 的素数时，$(p-1)!+1\geqslant 2(p-1)>p$，而由定理 2 又可知 $p\mid((p-1)!+1)$，因此 $(p-1)!+1$ 是复合数，即有无穷多个自然数 n 使 $n!+1$ 为复合数. 但我们并不知道是否有无穷多个自然数 n 使 $n!+1$ 为素数. 类似地，我们也不知道是否有无穷多个自然数 n 使 $n!-1$ 为素数.

记 p_i 为第 i 个素数. 例如 $p_1=2$, $p_2=3$, $p_3=5$, $\cdots$. 那末，是否存在无穷多个自然数 n 使 $q_n=p_1p_2\cdots p_n+1$ 为素数呢？或者，存在无穷多个自然数 n 使 q_n 为复合数？这些问题都没有解决. 例如 $p_1+1=3$, $p_1p_2+1=7$, $p_1p_2p_3+1=31$, $p_1p_2p_3p_4+1=211$, $p_1p_2p_3p_4p_5+1=2,311$ 都是素数，但当 $n=6, 7, 8$ 时，$p_1p_2\cdots p_n+1$ 可以分别被 59, 19, 347 整除，所以都是复合数.

§10. 表素数为两个自然数的平方和

引理 1. 假定 $p=4k+1$ 是素数，那末 $p\left|\left(\left(\frac{p-1}{2}\right)!^2+1\right)\right.$.

[1] C. E. Fröberg, Investigation of the Wilson remainders in the interval $3\leqslant p\leqslant 50,000$, *Ark. Mat.*; **4** (1963), 479～499.

证　因 $p=4k+1$，所以 $\frac{p-1}{2}=2k$ 是偶数，从而

$$(-1)(-2)\cdots\left(-\frac{p-1}{2}\right)=(-1)^{2k}1\cdot 2\cdot\cdots\cdot\frac{p-1}{2}$$
$$=1\cdot 2\cdot\cdots\cdot\frac{p-1}{2}.$$

因此

$$(p-1)(p-2)\cdots\left(p-\frac{p-1}{2}\right)\equiv(-1)(-2)\cdots\left(-\frac{p-1}{2}\right)$$
$$\equiv 1\cdot 2\cdot\cdots\cdot\frac{p-1}{2}\pmod p,$$

即

$$\frac{p+1}{2}\left(\frac{p+1}{2}+1\right)\cdots(p-1)\equiv 1\cdot 2\cdot\cdots\cdot\frac{p-1}{2}\pmod p.$$

$\left(\text{注意 } p-\frac{p-1}{2}=\frac{p+1}{2}\text{ 等}\right)$. 由此推出

$$(p-1)!\equiv\left(\frac{p-1}{2}\right)!^2\pmod p.$$

$\left(\text{注意 }\frac{p-1}{2}+1=\frac{p+1}{2}\right)$. 从而

$$(p-1)!+1\equiv\left(\frac{p-1}{2}\right)!^2+1\pmod p.$$

由定理 9.2 可知上式左端 $\equiv 0\pmod p$，所以

$$\left(\frac{p-1}{2}\right)!^2+1\equiv 0\pmod p.$$

引理证完.

引理 2. 假定 p 是素数，a 是整数，且 $p\nmid a$，那末存在适合于 $x<\sqrt{p}$ 与 $y<\sqrt{p}$ 的自然数 x, y 使

$$ax+y\equiv 0\pmod p\quad\text{或}\quad ax-y\equiv 0\pmod p.$$

证　用 m 表示 $\leqslant\sqrt{p}$ 的最大自然数. 所以 $m+1>\sqrt{p}$，即得 $(m+1)^2>p$. 当 x 与 y 分别跑过 0, 1, …, m 时，$ax-y$

共取 $(m+1)^2$ 个值. 因为 $(m+1)^2>p$, 所以用 p 来除这 $(m+1)^2$ 个 $ax-y$, 至少有两个的余数是相同的. 假定这两个是 ax_1-y_1 与 ax_2-y_2, 其中 $x_1\geqslant x_2$, 并且 (x_1, y_1) 与 (x_2, y_2) 是不同的, 即 $x_1=x_2$ 与 $y_1=y_2$ 不同时成立. 所以

$$ax_1-y_1\equiv ax_2-y_2 \pmod p, \quad x_1\geqslant x_2,$$

$$a(x_1-x_2)-(y_1-y_2)\equiv 0 \pmod p. \tag{1}$$

现在来证明 $x_1\neq x_2$. 如果 $x_1=x_2$, 那末由 (1) 式得 $y_1-y_2\equiv 0 \pmod p$. 但因为 $0\leqslant y_1\leqslant m<p$, $0\leqslant y_2\leqslant m<p$, 所以必须 $y_1=y_2$. 这与 ax_1-y_1 及 ax_2-y_2 的定义相矛盾. 同样, 如果 $y_1=y_2$, 那末

$$a(x_1-x_2)\equiv 0 \pmod p.$$

因 $p\nmid a$, 所以由引理 2.2 得 $p\mid(x_1-x_2)$. 同理可知 $x_1=x_2$. 这也与 ax_1-y_1 及 ax_2-y_2 的定义相矛盾. 所以 $x_1>x_2$, $y_1\neq y_2$. 取

$$x_1-x_2=x.$$

那末 $0<x\leqslant m\leqslant\sqrt{p}$. 因 $\sqrt{p}$ 不是整数 (不然, 素数 p 就是整数的平方了, 这不可能), 所以 $0<x<\sqrt{p}$. 又取

$$y=\begin{cases} y_1-y_2, & \text{当 } y_1>y_2, \\ y_2-y_1, & \text{当 } y_1<y_2, \end{cases}$$

那末 $0<y<\sqrt{p}$. 因此用上述 x, y 代入(1)式, 即可知

$$ax-y\equiv 0 \pmod p \quad \text{或} \quad ax+y\equiv 0 \pmod p.$$

引理证完.

定理 1(费马). 每一个形如 $p=4k+1$ 的素数都可以表示成两个自然数的平方和.

证 取 $a=\left(\frac{p-1}{2}\right)!$. 由于 a 的素因数都 $\leqslant\frac{p-1}{2}$, 所以 $p\nmid a$, 因此由引理 2 可知存在自然数 $x<\sqrt{p}$ 及 $y<\sqrt{p}$ 使

$$ax+y\equiv 0\pmod p \quad 或 \quad ax-y\equiv 0\pmod p.$$

总之

$$a^2x^2-y^2\equiv(ax+y)(ax-y)\equiv 0\pmod p. \tag{2}$$

由引理1可知

$$a^2\equiv -1\pmod p, \tag{3}$$

所以由(2)，(3)即得

$$0\equiv a^2x^2-y^2\equiv -x^2-y^2\pmod p,$$

换句话说

$$x^2+y^2=kp,$$

其中 k 是一个自然数．因为 $0<x<\sqrt{p}$，$0<y<\sqrt{p}$，所以 $k=1$．定理证完．

定理2．如果不计次序，那末将素数 p 表为两个自然数的平方和的方法是唯一的．

证　假定 p 有两种表为自然数的平方和的方法，即

$$p=x^2+y^2=x_1^2+y_1^2.$$

那末

$$\begin{aligned}p^2&=(x^2+y^2)(x_1^2+y_1^2)\\&=(xx_1+yy_1)^2+(xy_1-x_1y)^2\\&=(xx_1-yy_1)^2+(xy_1+x_1y)^2.\end{aligned} \tag{4}$$

另一方面

$$\begin{aligned}(xx_1+yy_1)(xy_1+x_1y)&=(x^2+y^2)x_1y_1+(x_1^2+y_1^2)xy\\&=p(xy+x_1y_1).\end{aligned} \tag{5}$$

由(5)可知

$$p\mid(xx_1+yy_1) \quad 或 \quad p\mid(xy_1+x_1y).$$

假定 $p\mid(xx_1+yy_1)$，那末 $xx_1+yy_1=kp$，其中 k 是自然数．代入(4)式第二个等式得

$$p^2=k^2p^2+(xy_1-x_1y)^2,$$

所以必须 $k=1$，即

$$(6)\qquad p=xx_1+yy_1.$$

且

$$(7)\qquad xy_1-x_1y=0.$$

因此由(6)，(7)得

$$px=x^2x_1+xy_1y=x^2x_1+y^2x_1=(x^2+y^2)x_1=px_1.$$

即得

$$x=x_1.$$

代入(7)式得

$$y=y_1.$$

现在假定 $p|(xy_1+x_1y)$. 代入(4)式的第三个等式得

$$(8)\qquad p=xy_1+x_1y.$$

与

$$(9)\qquad xx_1-yy_1=0.$$

因此由(8)，(9)得

$$px=x^2y_1+xx_1y=x^2y_1+y^2y_1=(x^2+y^2)y_1=py_1.$$

即得

$$x=y_1.$$

代入(9)式得

$$y=x_1.$$

总之，p 的两种表示法是一致的. 定理证完.

2 只有一种方法表示成两个自然数的平方和，即 $2=1^2+1^2$. 现在要问，形状是 $4k+3$ 的素数能否也表示为两个自然数的平方和呢？答案是否定的. 这是因为

$$z^2\equiv\begin{cases}0 \pmod 4), & \text{当 } 2|z,\\ 1 \pmod 4), & \text{当 } 2\nmid z,\end{cases}$$

所以

$$x^2+y^2\equiv\begin{cases}0(\bmod 4), & \text{当 } 2|x,\ 2|y,\\ 1(\bmod 4), & \text{当 } 2|x,\ 2\nmid y \text{ 或 } 2\nmid x,\ 2|y,\\ 2(\bmod 4), & \text{当 } 2\nmid x,\ 2\nmid y,\end{cases}$$

但是

$$4k+3\equiv 3(\bmod 4),$$

因此

$$x^2+y^2\not\equiv 4k+3(\bmod 4).$$

所以不仅是形如 $4k+3$ 的素数，而且形如 $4k+3$ 的自然数都不能表示成两个自然数的平方和.

由定理 2 可知，如果一个自然数 n 有两种方法表示为两个自然数的平方和，那末 n 一定是复合数．例如 $2,501=1^2+50^2=10^2+49^2$，所以 2,501 是复合数.

将素数 p 表示为自然数的平方差的问题，比较容易．假定

$$p=x^2-y^2.$$

那末

$$p=(x+y)(x-y).$$

因为 p 的因数只有 1 与 p，所以必须

$$p=x+y,\quad 1=x-y.$$

从而

$$x=\frac{p+1}{2},\quad y=\frac{p-1}{2}.$$

因此，当 p 是奇素数时，我们得仅有的把 p 分解成自然数的平方差的表示法

$$p=\left(\frac{p+1}{2}\right)^2-\left(\frac{p-1}{2}\right)^2.$$

§11. 二次剩余

假定 m 是一个自然数. 如果$(n, m)=1$,且同余式

$$x^2\equiv n \pmod m$$

有解,我们就称 n 做模 m 的二次剩余. 如果上面的同余式没有解, n 就叫做模 m 的二次非剩余.

我们可以将与 m 互素,且不超过 m 的自然数分成二类. 一类是模 m 的二次剩余,一类是模 m 的二次非剩余.

例如1, 2, 4是模7的二次剩余, 而3, 5, 6是模7的二次非剩余. 又如1, 3, 4, 9, 10, 12是模13的二次剩余, 而2, 5, 6, 7, 8, 11是模13的二次非剩余.

当 $p=2$ 时, $1^2\equiv 1 \pmod 2$, 所以每一个奇数都是模2的二次剩余. 今后假定 $p>2$ 为奇素数,我们有下述定理.

定理 1. 在 $1, 2, \cdots, p-1$ 中,共有 $\frac{1}{2}(p-1)$个模 p 的二次剩余,$\frac{1}{2}(p-1)$个模 p 的二次非剩余,且

$$1^2, 2^2, \cdots, \left(\frac{1}{2}(p-1)\right)^2 \tag{1}$$

用 p 除所得的余数,就是模 p 的全体二次剩余.

证　用 p 除(1)中各数所得的余数,显然都是模 p 的二次剩余. 现在要证明的是: $1, 2, \cdots, p-1$ 中,模 p 的二次剩余也就是这些. 假定 $1\leqslant n<p$. 如果同余式

$$x^2\equiv n \pmod p, \quad 1\leqslant x\leqslant p-1 \tag{2}$$

有解,那末由定理9.1可知它至多有二个解. 由

$$(p-x)^2\equiv(-x)^2\equiv x^2\equiv n \pmod p$$

可知(2)还有一个解 $p-x$. 如果 $\frac{1}{2}(p-1)<x\leqslant p-1$, 那末 $1\leqslant p-x\leqslant\frac{1}{2}(p-1)$. 因此如果(2)有解, 它总会有一个解适合于

$$1\leqslant x\leqslant\frac{1}{2}(p-1). \tag{3}$$

换句话说, 如果 n 是模 p 的二次剩余, 那末 n 必定模 p 同余于(1)中的一个数. 因此剩下来要证明的就是 n 中是模 p 的二次剩余恰有 $\frac{1}{2}(p-1)$ 个, 这只要证(1)中的任何两个数模 p 都互不同余. 假定 a^2, b^2 是(1)中的任何二数, 且 $a>b$. 如果

$$a^2\equiv b^2(\bmod p),$$

即得

$$p\mid(a+b)(a-b).$$

由引理 2.2 可知 $p\mid(a+b)$ 或 $p\mid(a-b)$, 但 $1\leqslant a+b<p$, $1\leqslant a-b<p$, 这是不可能的. 因此(1)中任何二数都模 p 互不同余. 定理证完.

定理 2(欧拉). 有关系式

$$n^{\frac{p-1}{2}}\equiv\begin{cases}1(\bmod p), & \text{当 } n \text{ 是模 } p \text{ 的二次剩余},\\ -1(\bmod p), & \text{当 } n \text{ 是模 } p \text{ 的二次非剩余}.\end{cases}$$

证 假定 n 是模 p 的二次剩余, 那末同余式

$$x^2\equiv n(\bmod p)$$

有解 x, 即 $p\mid(x^2-n)$. 所以由

$$\begin{aligned}x^{p-1}-n^{\frac{p-1}{2}}&=\left((x^2)^{\frac{p-1}{2}}-n^{\frac{p-1}{2}}\right)\\&=(x^2-n)\left((x^2)^{\frac{p-1}{2}-1}+(x^2)^{\frac{p-1}{2}-2}n+\cdots\right.\\&\qquad\left.+x^2n^{\frac{p-1}{2}-2}+n^{\frac{p-1}{2}-1}\right),\end{aligned}$$

可知

$$p \mid (x^{p-1}-n^{\frac{p-1}{2}}).$$

由定理 8.1 可知 $p \mid (x^{p-1}-1)$. 因此

$$p \mid (x^{p-1}-1-x^{p-1}+n^{\frac{p-1}{2}}).$$

即

$$n^{\frac{p-1}{2}} \equiv 1 \pmod{p}. \tag{4}$$

由定理 9.1 可知同余式(4)的解数不超过 $\frac{p-1}{2}$. 再由定理 1 和上面证明的事实可知它正好有 $\frac{p-1}{2}$ 个解, 即模 p 的 $\frac{p-1}{2}$ 个二次剩余. 所以若 n 是模 p 的二次非剩余, 必然不适合(4), 即 $p \nmid (n^{\frac{p-1}{2}}-1)$. 但是由引理 8.1 可知

$$p \mid (n^{p-1}-1)=(n^{\frac{p-1}{2}}-1)(n^{\frac{p-1}{2}}+1),$$

所以由引理 2.2 可知 $p \mid (n^{\frac{p-1}{2}}+1)$, 即

$$n^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

定理证完.

对于复合数 m, 定理 1 是不对的. 例如 $m=8$, 模 8 的二次剩余只有 1, 其余 3, 5, 7 都是模 8 的二次非剩余. 又如 $m=15$, 模 15 的二次剩余只有 1, 4, 其余 2, 7, 8, 11, 13, 14 都是模 15 的二次非剩余.

假定 $k>2$. 我们还可以类似地来定义模 m 的 k 次剩余与模 m 的 k 次非剩余如下: 如果 $(n, m)=1$, 且同余式

$$x^k \equiv n \pmod{m}$$

有解, 我们就叫 n 做模 m 的 k 次剩余. 如果上面的同余式没有解, 我们就叫 n 做模 m 的 k 次非剩余.

§ 12. 素数的出现概率为零

在前面几节中，我们所讲的一些素数的性质，都是初等的算术性质．但与素数有关的重要而深刻的结果，却都是通过分析工具而得到的．素数论中真正引人注目的问题往往也是用分析语言提出来的．所以在下面，我们将假定读者已经熟习有理数、实数与 x 的自然对数 $\ln x$ 的含义，并且学过极限与普通微积分，也熟习一些分析的常用记号．在用到这方面的普通知识时，我们就不作解释了．在这一部分我们仅仅把问题与结果作一个大概的介绍，证明就不写了．有兴趣的读者可以查阅有关的专著．

命 x 表示实数 x 的整数部分，即不大于 x 的最大整数．例如 $[1.5]=1$, $[0.1]=0$, $[-3.2]=-4$ 等．显然有

$$[x]\leqslant x<[x]+1.$$

设 N 是一个正整数，那末不超过 N 而又是整数 d 的倍数的正整数个数显然等于 $\left[\frac{N}{d}\right]$．以 $\pi(N)$ 表示不超过 N 的素数的个数．例如 $\pi(10)=4$, $\pi(20)=8$, $\pi(30)=10$ 等．又假定

$$2=p_1<p_2<\cdots<p_n\leqslant\sqrt{N}$$

是不超过 $\sqrt{N}$ 的全体素数． p_r

引理 1．$\pi(N)$ 有如下的表达式

$$\pi(N)=N+r-1-\sum_{i=1}^{r}\left[\frac{N}{p_i}\right]+\sum_{1\leqslant i<j\leqslant r}\left[\frac{N}{p_ip_j}\right]-\sum_{1\leqslant i<j<k\leqslant r}\left[\frac{N}{p_ip_jp_k}\right]+\cdots+(-1)^r\left[\frac{N}{p_1p_2\cdots p_r}\right].$$

证　当 $1\leqslant l\leqslant k$ 时，我们用 $\binom{k}{l}=\dfrac{k(k-1)\cdots(k-l+1)}{l!}$ 表示 k 个东西中任意选取 l 个东西的选法数目.

由引理 4.1 可知，如果自然数 $n\leqslant N$，而又是复合数，那末 n 必定被某 p_i 整除，此处 $1\leqslant i\leqslant r$. 不超过 N，而又是 p_i 的倍数的整数个数是 $\left[\dfrac{N}{p_i}\right]$，这些整数除了 p_i 本身是素数外，当然都是复合数，所以在计算 $\pi(N)$ 时，需先从 N 中减去这些复合数的个数，即减去

$$\sum_{i=1}^{r}\left(\left[\frac{N}{p_i}\right]-1\right)=\sum_{i=1}^{r}\left[\frac{N}{p_i}\right]-r.$$

但若一个整数，同时是 p_i 与 $p_j(i\neq j)$ 的倍数时，共被减去了二次，所以我们又必须添上一次，因此需加上

$$\sum_{1\leqslant i<j\leqslant r}\left[\frac{N}{p_ip_j}\right]$$

个数．又如果一个数是 $p_ip_jp_k(i<j<k)$ 的倍数时，那末它被划去 $\binom{3}{1}=3$ 次，而又被添上了 $\binom{3}{2}=3$ 次，等于没减，所以必须再行减去，即共减去

$$\sum_{1\leqslant i<j<k\leqslant r}\left[\frac{N}{p_ip_jp_k}\right].$$

依次类推．如果 n 恰有 k 个 $\leqslant\sqrt{N}$ 的不同的素因子，那末共减去 $\binom{k}{1}+\binom{k}{3}+\cdots$ 次，共加上 $\binom{k}{2}+\binom{k}{4}+\cdots$ 次．而根据二项式定理，

$$-\binom{k}{1}+\binom{k}{2}-\binom{k}{3}+\binom{k}{4}-\cdots+(-1)^k\binom{k}{k}$$
$$=(1-1)^k-1=-1,$$

所以只被减去1次．另外由于1不是素数，所以还需从 N 中减去1．因此引理成立．

引理1的证明用了所谓"逐步淘汰原则"，这是一个很有用的方法．读者如有兴趣，可参阅华罗庚著《数论导引》第一章．

设 $\varphi(n)$ 表示不超过 n，而又与 n 互素的自然数个数，$\varphi(n)$ 就是所谓欧拉函数．例如 $\varphi(1)=1$，$\varphi(2)=1$，$\varphi(3)=2$ 等．一般说来，我们有

引理2． $$\varphi(n)=n\prod_{p|n}\left(1-\frac{1}{p}\right),$$

其中 $\prod_{p|n}\left(1-\frac{1}{p}\right)$ 表示 p 取 n 的所有不同素因数时，相应的 $1-\frac{1}{p}$ 的连乘积．

证　设 n 的标准分解式是

$$n=p_1^{a_1}\cdots p_r^{a_r}.$$

那末不与 n 互素就表示与 n 至少有一个公因数 p_i，此处 $1\leqslant i\leqslant r$，而不超过 n 又能被 p_i 整除的自然数个数为 $\frac{n}{p_i}$ $(1\leqslant i\leqslant r)$．在计算 $\varphi(n)$ 时，需从 n 中减去，即需减去 $\sum_{i=1}^{r}\frac{n}{p_i}$．但若 n 同时被 p_i 与 $p_j\,(i\neq j)$ 整除，那末这种数被减去了二次，所以需添上一次，即需添上 $\sum_{1\leqslant i<j\leqslant r}\frac{n}{p_ip_j}$．依次类推，得

$$\begin{aligned}\varphi(n)&=n-\sum_{i=1}^{r}\frac{n}{p_i}+\sum_{1\leqslant i<j\leqslant r}\frac{n}{p_ip_j}-\cdots+(-1)^r\frac{n}{p_1p_2\cdots p_r}\\&=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right)=n\prod_{p|n}\left(1-\frac{1}{p}\right).\end{aligned}$$

引理证完．

由定理3.1已知素数的个数有无穷多．即 $\pi(N)\to\infty$（当

$N\to\infty$). 但不超过 N 的素数个数 $\pi(N)$ 与 N 的比 $\frac{\pi(N)}{N}$ 的分布情形又如何呢? 如果 $\lim\limits_{N\to\infty}\frac{\pi(N)}{N}$ 存在, 我们就称它做素数的"出现概率". 我们将证明:

定理 1. 素数的出现概率为 0, 即

$$\lim_{N\to\infty}\frac{\pi(N)}{N}=0.$$

由于不超过 N 的复合数个数是 $N-\pi(N)-1$, 所以由定理 1 立即推出复合数的出现概率是 1, 即

$$\lim_{N\to\infty}\frac{N-\pi(N)-1}{N}=1.$$

用数论的术语来说就是"几乎所有"的数都不是素数, 而是复合数.

在证明定理 1 之前, 我们再证明两条引理.

引理 3. 级数 $\sum\limits_{n=1}^{\infty}\frac{1}{n}$ 发散.

证 $$\sum_{n=1}^{2^t}\frac{1}{n}=1+\frac{1}{2}+\left(\frac{1}{3}+\frac{1}{4}\right)+\left(\frac{1}{5}+\cdots+\frac{1}{8}\right)$$
$$+\cdots+\left(\frac{1}{2^{t-1}+1}+\cdots+\frac{1}{2^t}\right)$$
$$>1+\frac{1}{2}+\left(\frac{1}{4}+\frac{1}{4}\right)+\left(\frac{1}{8}+\cdots+\frac{1}{8}\right)$$
$$+\cdots+\left(\frac{1}{2^t}+\cdots+\frac{1}{2^t}\right)$$
$$=1+\frac{1}{2}+\frac{1}{2}+\cdots+\frac{1}{2}$$
$$=1+\frac{t}{2}\to\infty\ (\text{当 } t\to\infty).$$

引理证完.

引理4. 无穷乘积 $\prod_p\left(1-\frac{1}{p}\right)=0$，此处 p 通过所有的素数.

证 如果引理不成立. 由于 $1>1-\frac{1}{p}>0$，所以

$$\prod_p\left(1-\frac{1}{p}\right)=a>0.$$

从而

$$\frac{1}{a}=\prod_p\left(1-\frac{1}{p}\right)^{-1}.$$

记 $N=2^t$，这儿 $t=2\left(\left[\frac{1}{a}\right]+1\right)$. 所以由引理3的证明即得

$$\frac{1}{a}=\prod_p\left(1-\frac{1}{p}\right)^{-1}>\prod_{p\leqslant N}\left(1-\frac{1}{p}\right)^{-1}$$

$$=\prod_{p\leqslant N}\left(\sum_{i=0}^{\infty}\frac{1}{p^i}\right)>\sum_{n=1}^{N}\frac{1}{n}>1+\frac{t}{2}$$

$$=\left[\frac{1}{a}\right]+2>\frac{1}{a}+1,$$

即 $\frac{1}{a}>\frac{1}{a}+1$. 这是不可能的，因此引理成立.

定理1的证明. 与引理1的证明相仿可知，不超过 N 的自然数中不能被前 s 个素数整除的整数个数 $\pi(N, s)$ 等于

$$\pi(N, s)=N-\sum_{i=1}^{s}\left[\frac{N}{p_i}\right]+\sum_{1\leqslant i<j\leqslant s}\left[\frac{N}{p_ip_j}\right]$$

$$-\cdots+(-1)^s\left[\frac{N}{p_1p_2\cdots p_s}\right]$$

(注意其中 p_s 不一定表示 $\leqslant\sqrt{N}$ 的最大素数). 由于大于 p_s，而又不超过 N 的素数不能被前 s 个素数整除，所以

$$\pi(N)\leqslant s+\pi(N, s).$$

由于 $x-1<[x]<x+1$, 所以

$$\pi(N)<s+N\left(1-\sum_{i=1}^{s}\frac{1}{p_i}+\sum_{1\leqslant i<j\leqslant s}\frac{1}{p_ip_j}\right.$$

$$\left.+\cdots+(-1)^s\frac{1}{p_1p_2\cdots p_s}\right)$$

$$+\left(\sum_{i=1}^{s}1+\sum_{1\leqslant i<j\leqslant s}1+\cdots+\sum_{1\leqslant i_1<\cdots<i_{s-1}\leqslant s}1+1\right).$$

由于

$$\sum_{i=1}^{s}1=s,\quad \sum_{1\leqslant i<j\leqslant s}1=\binom{s}{2},\cdots,\quad \sum_{1\leqslant i_1<\cdots<i_{s-1}\leqslant s}1=\binom{s}{s-1},$$

所以

$$\sum_{i=1}^{s}1+\sum_{1\leqslant i<j\leqslant s}1+\cdots+\sum_{1\leqslant i_1<\cdots<i_{s-1}\leqslant s}1+1<1+\binom{s}{1}+\binom{s}{2}$$

$$+\cdots+\binom{s}{s-1}+1=2^s.$$

因此

$$\pi(N)<N\prod_{i=1}^{s}\left(1-\frac{1}{p_i}\right)+2^s+s$$

$$<N\prod_{i=1}^{s}\left(1-\frac{1}{p_i}\right)+2^{s+1}.$$

取 $s+1=\left[\frac{\ln N}{2\ln 2}\right]$. 代入上式即得

$$0<\frac{\pi(N)}{N}<\prod_{i=1}^{\left[\frac{\ln N}{2\ln 2}\right]-1}\left(1-\frac{1}{p_i}\right)+\frac{2^{\frac{\ln N}{2\ln 2}}}{N}$$

$$=\prod_{i=1}^{\left[\frac{\ln N}{2\ln 2}\right]-1}\left(1-\frac{1}{p_i}\right)+\frac{1}{\sqrt{N}}.$$

当 $N\to\infty$ 时, 由引理 4 即得

$$\lim_{N\to\infty}\frac{\pi(N)}{N}=0.$$

定理证完.

注意：由引理 4 即可推知 $\pi(N)\to\infty$(当 $N\to\infty$). 事实上，如果 $\pi(N)$ 有限，那末 $\prod_p\left(1-\frac{1}{p}\right)$ 只有有限项相乘，所以不能是零. 但这一证明远较 §3 的方法得到的东西为多. 由它可以得到 $\pi(N)$ 的一个粗略估计. 这里介绍的方法是属于欧拉的.

§13. 素数定理

在作进一步讨论之前，我们先引进几个近代素数论中常用的记号

$$\ll,\ O,\ o,\ \sim.$$

它们的含义解释如下：设 x 是一个连续趋于无穷的变量. 又设 $\varphi(x)$ 是 x 的正值函数，$f(x)$ 是任意函数. 如果有一个与 x 无关的正常数 A 使

$$|f(x)|\leqslant A\varphi(x)$$

成立，我们就记为

$$f(x)\ll\varphi(x),\quad \text{或}\quad f(x)=O(\varphi(x)).$$

这里常数 A 称为与"$\ll$"或"O"有关的常数. 如果 $f(x)-g(x)\ll\varphi(x)$，我们常常记为

$$f=g+O(\varphi)$$

更为方便一些. 又如果

$$\lim_{x\to\infty}\frac{f(x)}{\varphi(x)}=0\quad \text{或}\quad 1,$$

我们就分别记为

$$f(x)=o(\varphi(x)) \quad 或 \quad f(x)\sim\varphi(x).$$

例如 $\sin x\ll 1$，$x+\frac{1}{x}\ll x\ll x+\frac{1}{x}$，$x+\frac{1}{x}=o(x^2)$，$x+\sin x\sim x$ 或 $x+\sin x=x+o(1)$ 等.

由于

$$e^x=1+x+\cdots+\frac{x^n}{n!}+\frac{x^{n+1}}{(n+1)!}+\cdots$$

所以

$$e^x x^{-n}>\frac{x}{(n+1)!},$$

此处 n 为任意正整数. 即 e^x 趋于无穷较 x 之任何整数次方幂为快, 或谓 e^x 之无穷大阶大于 x^n 之阶. 用上面的记号可以记为

$$x^n=o(e^x).$$

若 α 为任何正数, 则仍有

$$x^\alpha=O(x^{[\alpha]+1})=o(e^x).$$

以 $\ln y$ 代入上式之 x, 则

$$(\ln y)^\alpha=o(y),$$

即得

$$\ln x=o(x^\delta),$$

此处 δ 为任意正数. 换言之，$\ln x$ 之无穷大阶较 x 之任何正数方幂为小. 同理 $\ln\ln x$ 的无穷大阶比 $\ln x$ 的任何正数方幂为小. 又记

$$\mathrm{li}\,x=\lim_{\eta\to 0}\left(\int_0^{1-\eta}+\int_{1-\eta}^{x}\right)\frac{dt}{\ln t}.$$

那末

$$\lim_{x\to\infty}\frac{\mathrm{li}\,x}{\dfrac{x}{\ln x}}=\lim_{x\to\infty}\frac{(\mathrm{li}\,x)'}{\left(\dfrac{x}{\ln x}\right)'}=\lim_{x\to\infty}\frac{\dfrac{1}{\ln x}}{\dfrac{1}{\ln x}-\dfrac{1}{(\ln x)^2}}=1,$$

即

$$\operatorname{li} x \sim \frac{x}{\ln x}.$$

当然在这些定义中，我们可以假定 x 是通过某一数列趋于无穷的，例如通过自然数列趋于无穷等．我们还可以将“趋于无穷”换成“趋于限 l”，这儿 l 是一个有限数．例如当 $x\to 0$ 时有 $x+x^2=O(x)$，$\sin x\sim x$，$x=o(1)$等．但在以后，我们只用到趋于无穷的情况．

素数论中许多著名的猜想，都是从经验概括出来的．然后再经过严格的数学推导，设法加以证明．例如关于 $\pi(x)$，我们有下面的表．

x	$\pi(x)$	$\frac{x}{\ln x}$	$\operatorname{li} x$	$\frac{\pi(x)}{\operatorname{li} x}$	$\frac{\pi(x)}{x}$
1,000	168	145	178	0.94	0.1680
10,000	1,229	1,086	1,246	0.98	0.1229
50,000	5,133	4,621	5,167	0.993	0.1026
100,000	9,592	8,686	9,630	0.996	0.0959
500,000	41,538	38,103	41,606	0.9983	0.0830
1,000,000	78,498	72,382	78,628	0.9983	0.0785
2,000,000	148,933	137,848	149,055	0.9991	0.0745
5,000,000	348,513	324,149	348,638	0.9996	0.0697
10,000,000	664,579	620,417	664,918	0.9994	0.0665
20,000,000	1,270,607	1,189,676	1,270,905	0.9997	0.0635
90,000,000	5,216,954	4,913,897	5,217,810	0.99983	0.0580
100,000,000	5,761,455	5,428,613	5,762,209	0.99986	0.0576
1,000,000,000	50,847,478	48,254,630	50,849,235	0.99996	0.0508

从 $\pi(x)$ 的最初几个函数值看来,$\pi(x)$ 似乎很不规则,但是随着数据的增加,从表中可以看到,对于 $\pi(x)$ 可能有 1) $\pi(x)\to\infty$(当 $x\to\infty$),即素数有无穷多,2) $\frac{\pi(x)}{x}\to 0$(当 $x\to\infty$),即"几乎所有"的自然数都是复合数. 这两点我们在§3与§12中已经证明过了. 更进一步,$\pi(x)$ 还可能有一个渐近表达式. 勒让德 (A. M. Legendre) 在 1830 年猜想,当 $x\to\infty$ 时,

$$\pi(x)\sim\frac{x}{\ln x-B},$$

其中 $B=1.08366$. 高斯又独立地建议了一个类似的,但并不与它相等的公式. 以一千个相继自然数为单位,高斯的方法在于计算每个单位中的素数个数,他建议用函数 $\frac{1}{\ln x}$ 来表示在充分大的整数 x 附近的素数分布的平均密度("单位区间中素数的百分率"). 因此高斯猜想

$$\pi(x)\sim \operatorname{li} x.$$

如果我们仅仅只考虑主阶,由于

$$\lim_{x\to\infty}\frac{\dfrac{x}{\ln x-1.08366}}{\dfrac{x}{\ln x}}=1 \quad 及 \quad \lim_{x\to\infty}\frac{\operatorname{li} x}{\dfrac{x}{\ln x}}=1,$$

所以我们可以将这两个猜想写为

$$\pi(x)\sim\frac{x}{\ln x},$$

这就是通常所称的"素数定理". 这是素数分布理论的中心定理. 近百年来,决定素数定理是否正确的问题,吸引了很多优秀数学家的注意.

首先对这个问题作出重要贡献的是车比雪夫 (П. Л.

Чебышев). 他在 1848 年与 1950 年证明了:

定理 1(车比雪夫). 有关系式

$$a \leqslant \varliminf_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} \leqslant 1 \leqslant \varlimsup_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} \leqslant \frac{6}{5}a,$$

这儿 $a=0.92129$.

由定理 1 显然推出 $\frac{\pi(x)}{x}\to 0$(当 $x\to\infty$). 由定理 1 可以看出, 如果当 $x\to\infty$ 时, $\frac{\pi(x)}{\frac{x}{\ln x}}$ 的极限存在, 那末极限必定是 1, 而且对于一切 $x\geqslant 2$, $\frac{\pi(x)}{\frac{x}{\ln x}}$ 一定位于两个正常数之间. 尽管定理 1 中的常数 a 不断地被以后的数学家加以改进, 但并不能导致问题的最终解决, 即完全证明素数定理.

关于素数定理, 赛尔凡斯特(J. J. Sylvester)曾用下面的话表明他对这个问题的展望.

"但是要确定这种可能性的存在,我们或许要等待在世界上产生这样一个人,他的智慧与洞察力象车比雪夫一样,证明自己是超人一等的".

但就在赛尔凡斯特说这些话时出生的阿达玛 (J. Hadamard), 依赖于前人特别是黎曼 (B. Riemann)的工作,用复变函数论的方法,在 1896 年证明了素数定理. 几乎同时而又独立地证明了这个定理的还有达拉瓦勒布桑(C. J. de la Vallée Poussin).

定理 2(素数定理). $\pi(x)\sim\frac{x}{\ln x}$.

由定理 2 立刻可以推出

定理 3. 设 p_n 表示第 n 个素数，那末

$$p_n \sim n \ln n.$$

证　在定理 2 中取 $x=p_n$ 得

$$n=\pi(p_n)\sim\frac{p_n}{\ln p_n},$$

即

$$p_n \sim n \ln p_n.$$

由于 $\ln\ln p_n=o(\ln p_n)$，所以

$$\ln p_n \sim \ln n+\ln\ln p_n \sim \ln n,$$

代入上式即得定理 3.

寻求一个“素数定理”的初等证明，即不用复变函数论或类似工具的证明，是素数论中历时很久的难题之一．这一初等证明直到 1949 年，才由赛尔贝尔格(A. Selberg)与爱多士(P. Erdös)独立得到．有兴趣阅读车比雪夫定理与素数定理证明的读者，请看华罗庚著《数论导引》第五章与第九章.

§ 14. 素数定理的误差项

达拉瓦勒布桑在 1899 年证明了：

定理 1(达拉瓦勒布桑).

$$\pi(x)-\mathrm{li}\,x=O\left(xe^{-a\sqrt{\ln x}}\right), \tag{1}$$

这儿 $a>0$ 是一个常数.

由分部积分可得

$$\mathrm{li}\,x=\frac{x}{\ln x}+\frac{x}{(\ln x)^2}+\cdots+(n-1)!\frac{x}{(\ln x)^n}+O\left(\frac{x}{(\ln x)^{n+1}}\right). \tag{2}$$

另一方面

$$(3)\qquad \frac{x}{\ln x-B}=\frac{x}{\ln x}+\frac{Bx}{(\ln x)^2}+\cdots+\frac{B^{n-1}x}{(\ln x)^n}+O\left(\frac{x}{(\ln x)^{n+1}}\right).$$

由于$e^{-a\sqrt{\ln x}}=o\left(\frac{1}{(\ln x)^A}\right)$，此处$A>0$为任意常数，而与"$o$"有关的常数仅依赖于$a$与$A$，所以比较(1)，(2)，(3)即得

$$\pi(x)-\frac{x}{\ln x-B}=\begin{cases}O\left(\frac{x}{(\ln x)^2}\right), & \text{当 } B\neq 1,\\ O\left(\frac{x}{(\ln x)^3}\right), & \text{当 } B=1.\end{cases}$$

这说明在勒让德关于$\pi(x)$的猜测(见§13)中，取$B=1$最好，即取$\frac{x}{\ln x-1}$来逼近$\pi(x)$最好．但不管怎样，用高斯提出的用$\mathrm{li}\,x$来逼近$\pi(x)$，更为精密得多．

不少数学家改进了公式(1)的误差项．目前最好的结果是依·维诺格拉朵夫(И. М. Виноградов)与卡罗波夫(Н. М. Коробов)于1958年独立证明的．即：

定理2(依·维诺格拉朵夫-卡罗波夫)．

$$(4)\qquad \pi(x)-\mathrm{li}\,x=O\left(xe^{-(\ln x)^{3/5-\varepsilon}}\right),$$

其中ε是任意正常数，而与"O"有关的常数仅依赖于ε．

(4)式虽然比(1)式精密，但距离理想的猜想结果还相差很远．理想的猜想结果是

$$(5)\qquad \pi(x)-\mathrm{li}\,x=O(\sqrt{x}\ln x).$$

冯·柯赫(H. von Koch)在1901年曾在所谓黎曼猜测成立的情况下，证明了(5)式．由于黎曼猜测是用复变函数论的语言叙述的，在这里我们就不讲了．有兴趣的读者，请看华罗庚著

《指数和的估计及其在数论中的应用》第三章. 不过, 由(5)的成立, 也可以推出黎曼猜测的成立. 所以(5)式与黎曼猜测是等价的, 因此(5)式也可以看成是黎曼猜测的另一种形式. 特别应该指出, 素数论中许多著名问题的解决, 往往可以归结为黎曼猜测的证明. 所以断定这一猜测的成立与否, 在数论中实在是最为重要的了.

我们现在甚至还远远不能证明比(5)弱得多的结果, 即

$$\pi(x)-\mathrm{li}x=O(x^{1-\varepsilon}),\tag{6}$$

这儿 ε 是某一正数(例如 $\varepsilon=10^{-10,000}$), 而与“O”有关的常数仅依赖于 ε.

关于 $\pi(x)$ 与第 n 个素数 p_n, 罗素 (J. B. Rosser) 与熊飞尔德(L. Schoenfeld)[1] 证明了下面的不等式:

定理 3. 1) $\dfrac{x}{\ln x-\dfrac{3}{2}}<\pi(x)<\dfrac{x}{\ln x-\dfrac{1}{2}}$, 其中 $x\geqslant 67$,

2) $n\ln n<p_n<n(\ln n+\ln\ln n)$, 其中 $n\geqslant 6$.

§15. 素数定理误差项的不规则性

我们先引进记号“Ω”. 设 $\varphi(x)$ 是 x 的正值函数. 如果存在与 x 无关的正常数 c, 使有任意大的 x 满足

$$|f(x)|>c\varphi(x),$$

我们就用记号

$$f(x)=\Omega(\varphi(x))$$

来表示. 所以“Ω”是“O”的逆记号. 如果 $f(x)$ 是 x 的实函

[1] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.*; **6** (1962), 64~94.

数，即 $f(x)$ 仅取实值，且有任意大的 x 使 $f(x)>c\varphi(x)$，就记作

$$f(x)=\Omega_+(\varphi(x)).$$

又如果有任意大的 x 使 $f(x)<-c\varphi(x)$，就记作

$$f(x)=\Omega_-(\varphi(x)).$$

所以对于实函数，“Ω”等价于“或者 Ω_+， 或者 Ω_-”. 我们还用记号“$\Omega_\pm$”表示“Ω_+ 与 Ω_- 都成立”.

由 § 13 的表中可见，似乎应该有

$$\pi(x)<\operatorname{li} x. \tag{1}$$

例如 $\pi(10^9)<\operatorname{li} 10^9$. 但是李特伍德(J. E. Littlewood)在 1914 年证明了：

定理 1(李特伍德). 当 $x\to\infty$ 时，

$$\pi(x)-\operatorname{li} x=\Omega_\pm\left(\frac{x^{\frac{1}{2}}}{\ln x}\ln\ln\ln x\right).$$

从这个定理看出，可以找到任意大的 x 使(1)式成立，也可以找到任意大的 x 使(1)式不成立，即使

$$\pi(x)>\operatorname{li} x \tag{2}$$

成立. 但定理 1 纯粹是一个“存在定理”. 到底在多大的范围内，就能找到使 (2) 成立的 x 呢？定理 1 并不能回答. 直到 1933 年，斯克斯(S. Skewes)才首先证明了有自然数 x 适合于

$$x<10^{10^{10^{10^3}}},10^{10^{10^{34}}}$$

并使(2)成立. 莱莱将斯克斯的结果改进为：在 1.53×10^{1165} 与 1.65×10^{1165} 之间至少有 10^{500} 个整数使(2)式成立. 他并证明了，在不超过 10^{20} 的整数中，找不到使(2)成立的整数[1].

[1] D. H. Lehmer, On the difference $\pi(x)-\operatorname{li} x$, *Acta Arith*; 1966, 397～410.

§ 16. 相邻两素数之差

设 p_n 表示第 n 个素数，现在我们来研究相邻两素数 p_{n+1} 与 p_n 的差

$$d_n=p_{n+1}-p_n$$

的分布问题.

有所谓贝特朗(J. Bertrand)假设，即对于任何自然数 $m>3$，在 m 与 $2m-2$ 之间一定有一个素数. 这一著名假设是车比雪夫在 1850 年解决的. 取 $m=p_n(n\geqslant3)$. 则由贝特朗假设可知 $p_{n+1}<2m-2$，所以

$$d_n<2m-2-m=m-2=p_n-2.$$

因此这一结果远较定理 3.2 精密. 但另一方面，此定理的精确性并不算好，还有更精密的结果(见 1).

关于 d_n 的重要问题与结果，有下面这些.

1) 最重要的是设法找函数 $f_1(n)$ 与 $f_2(n)$ 使

$$d_n\leqslant f_1(n)$$

与

$$d_n\geqslant f_2(n)$$

对于所有充分大的 n 成立.

由目前具有最精密误差项的素数定理(定理 14.2)只能推出

(1) $$f_1(n)=p_ne^{-(\ln p_n)^{3/5-\varepsilon}}.$$

需假定黎曼猜测成立，即由公式(15.5)(即 § 15，公式(15))才能得到

(2) $$f_1(n)=cp_n^{1/2}\ln p_n.$$

首先是霍海赛尔(G. Hoheisel)证明了:

(3) $$f_1(n)=cp_n^{\frac{32999}{33000}}.$$

当然(3)比(1)强多了. 不少数学家改进了霍海赛尔的结果. 目前最好的结果是霍斯勒证明的. 他得到了:

定理 1(霍斯勒)[1]. $d_n \ll p_n^{\frac{7}{12}+\varepsilon}$, 这儿 ε 是任意正常数, 而与"$\ll$"有关的常数仅依赖于 ε.

由定理 1 立刻推知, 对于任何 $\varepsilon>0$, 皆存在仅依赖于 ε 的常数 $n_0(\varepsilon)$, 当 $n>n_0$ 时, 在 n 与 $n+n^{\frac{7}{12}+\varepsilon}$ 之间恒存在一个素数. 这一结论远比贝特朗假设为优.

关于 $f_2(n)$, 我们还一无所知, 如果所谓孪生素数猜想正确, 就能得到

$$f_2(n)=2$$

(见 §19).

关于 $f_1(n)$ 的理想猜想结果, 从现有的素数表中看, 似乎应该是(2). 但数理统计学家克拉梅尔(H. Cramér), 借助一个以概率论为基础的富有启发性的方法推测, 甚至可能是

$$f_1(n)=(\ln p_n)^2.$$

2) 另一类问题是设法寻找函数 $f_3(n)$ 与 $f_4(n)$, 使对于无穷多个 n 有

$$d_n\leqslant f_3(n),$$

又对于无穷多个 n 有

$$d_n\geqslant f_4(n).$$

---

[1] M. N. Huxley, On the difference between consecutive primes, *Inv. Math.*; **15** (1972), 164～170.

我们有下面的结果:

定理 2(霍斯勒)[1].

$$f_3(n)=\left(\frac{1}{4}+\frac{\pi}{16}+\varepsilon\right)\ln p_n,$$

其中 ε 是任意正常数.

定理 3(兰肯 A. E. Rankin).

$$f_4(n)=\left(\frac{1}{3}-\varepsilon\right)\ln p_n\ln\ln p_n\frac{\ln\ln\ln\ln p_n}{(\ln\ln\ln p_n)^2},$$

其中 ε 是任意正常数.

3) 还有一类问题是寻找函数 $f_5(n)$, 使对于几乎所有的 n 都有

$$d_n\leqslant f_5(n),$$

即适合于 $n\leqslant x$ 的自然数 n 使上式成立的个数 $\sim x$. 还要寻找 $f_6(n)$, 使对于几乎所有的 n 都有

$$d_n\geqslant f_6(n)$$

我们有下面的结果:

定理 4(克拉梅尔). 在黎曼猜测真确的假定下有

$$f_5(n)=(\ln p_n)^3.$$

定理 5(帕拉哈 K. Prachar).

$$f_6(n)=\frac{\ln p_n}{g(p_n)},$$

其中 $g(x)$ 是任何递增且适合于 $g(x)\to\infty$ 与 $\frac{\ln x}{g(x)}\to\infty$ (当 $x\to\infty$) 的函数.

---

[1] M. N. Huxley, Small differences between consecutive primes, *Mathematika*; **2, 20** (1973), 229~232.

§ 17. 素数在算术级数中的分布

任何奇数一定 4 除余 1 或 4 除余 3. 因此可以将奇数按 4 除余 1 或 4 除余 3 分为二类:

(1) $$1, 5, 9, 13, 17, 21, \cdots$$

(2) $$3, 7, 11, 15, 19, 23, \cdots$$

我们在 § 3 与 § 8 已经证明了在数列 (1) 与 (2) 中都含有无穷多个素数(见定理 3.3 与定理 8.2). 现在要问对于一般的以自然数 l 为首项, 以自然数 $k(\geqslant l)$ 为公差的算术级数(或叫做等差级数).

(3) $$l, l+k, l+2k, l+3k, \cdots$$

中, 是不是都含有无穷多个素数呢?

如果 $(l, k)=d>1$, 那末 $d \mid (l+nk)$ $(n=0, 1, 2, \cdots)$, 所以除 l 可能是素数外, 算术级数(3)中的其他数都是复合数. 因此如果在数列(3)中有无穷多个素数, 就必需 $(l, k)=1$. 但是对于任何适合于 $(l, k)=1$ 的正整数 l, k, 算术级数(3)中是不是一定有无穷多个素数呢? 这一十分重要而又困难的问题是狄里赫勒 (P. G. Lejeune Dirichlet) 在 1837 年解决的. 答案是肯定的.

设 $\pi(x, k, l)$ 表示算术级数(3)中 $\leqslant x$ 的素数个数.

定理 1(狄里赫勒). 如果 $(l, k)=1$, 那末 $\pi(x, k, l)\to\infty$ (当 $x\to\infty$).

定理 1 原来的证明需要一些高深的数学知识, 它的"初等证明"也是赛尔贝尔格在 1949 年得到的. 有兴趣阅读定理 1 的初等证明的读者, 请看华罗庚著《数论导引》第九章.

设 $l_1, \cdots, l_{\varphi(k)}$ 是全体不超过 k，而与 k 互素的自然数，这儿 $\varphi(k)$ 是欧拉函数(见 §12)．现在提一个问题．问

$$\pi(x, k, l_1), \cdots, \pi(x, k, l_{\varphi(k)})$$

是不是都两两渐近地相等？即对于任何 $i \neq j$，关系式

$$\pi(x, k, l_i) \sim \pi(x, k, l_j)$$

是不是都成立？答案也是肯定的．这说明不超过 x 的素数在 $\varphi(k)$ 个算术级数 $l_i + nk$ $(1 \leqslant i \leqslant \varphi(k),\ n=0, 1, 2, \cdots)$ 中是“平均”分配的．不仅如此，用与 §14 相类似的方法还可以进一步证明：

定理 2． $\pi(x, k, l) = \dfrac{1}{\varphi(k)} \operatorname{li} x + O\left(xe^{-(\ln x)^{3/5-\varepsilon}}\right)$，$(l, k) = 1$，这儿 ε 是任意正常数，而与“O”有关的常数依赖于 k 与 ε.

与 $\pi(x)$ 一样，关于 $\pi(x, k, l)$ 的理想的猜想结果应该是：

$$\pi(x, k, l) = \frac{1}{\varphi(k)} \operatorname{li} x + O\left(x^{\frac{1}{2}} \ln x\right), \quad (l, k) = 1, \tag{4}$$

其中与“O”有关的常数与 k, l 无关．因为当 $k=1$ 时，$\pi(x, 1, 1) = \pi(x)$，所以要证明公式(4)比证明 (14.5) 更加困难．与 §16 相类似，我们还可以证明：

定理 3． 命 $p_n(k, l)$ 表示当 $(l, k) = 1$ 时，数列(3)中的第 n 个素数．那末

$$p_{n+1}(k, l) - p_n(k, l) = O\left(p_n(k, l)^{\frac{7}{12}+\varepsilon}\right),$$

其中 ε 是任何正常数，而与“O”有关的常数仅依赖于 k 与 ε.

定理 2 是对于固定的 k 而得到的．是不是有一个 $\pi(x, k, l)$ 的与 k 无关的渐近表示公式呢？这是很重要的问题，关于这个问题，济格尔(C. L. Siegel)证明了：

定理 4(济格尔)．设 l, k 是适合于 $(l, k) = 1$ 及 $3 \leqslant k \leqslant (\ln x)^K$ 的自然数，其中 K 是任意正常数，那末

$$\pi(x, k, l)=\frac{1}{\varphi(k)}\operatorname{li} x+O(xe^{-a\sqrt{\ln x}}),$$

这儿 $a>0$, 而与"O"有关的常数仅依赖于 K.

另一个有趣而重要的问题是如何估计算术级数 (3) 中的最小素数 $p_1(k, l)$的上界. 邱拉(S. Chowla)猜测, 当$(l, k)=1$ 时,对于任何 $\varepsilon>0$, 都有

$$p_1(k, l)=O(k^{1+\varepsilon}),$$

其中与"O"有关的常数仅依赖于 ε.

假定公式(4)成立,那末用 $x=k^{2+\varepsilon}$ 代入,容易推出

$$p_1(k, l)=O(k^{2+\varepsilon}),\quad (l, k)=1,$$

其中与"O"有关的常数仅依赖于 ε. 但公式(4)是未经证明的. 林尼克(Ю. В. Линник)首先迈出了重要的一步, 他证明了:

定理 5(林尼克). 当$(l, k)=1$ 时, $p_1(l, k)\ll k^c$, 这儿 c 是一个正常数.

我国数学家潘承洞首先证明了 c 是可以具体定出来的. 他证明了 $c\leqslant 5,448$. 我国数学家陈景润证明过 $c\leqslant 168$. 目前已发表的最佳结果是尤梯拉证明的 $c\leqslant 80$[1].

1965 年, 朋比尼(E. Bombieri)证明了下面关于 $\pi(x, k, l)$重要的中值公式:

定理 6(朋比尼)[2]. 对于任意常数 $A>0$, 都存在常数 $B>0$ 使

$$(5)\qquad \sum_{k\leqslant x^{1/2}/(\ln x)^B}\max_{(l, k)=1}\left|\pi(x, k, l)-\frac{\operatorname{li} x}{\varphi(k)}\right|=O\left(\frac{x}{(\ln x)^A}\right),$$

---

[1] Matti Jutila, On Linnik's Constant, *Math. Scand*; **41** (1977), 45～62.

[2] E. Bombieri, On the Large Sieve, *Mathematika*; **12**, **2** (1965), 201～225.

这儿$\max\limits_{(l,k)=1}\left|\pi(x,k,l)-\frac{\operatorname{li}x}{\varphi(k)}\right|$表示适合于$(l,k)=1$的$\varphi(k)$个$\left|\pi(x,k,l)-\frac{\operatorname{li}x}{\varphi(k)}\right|$中最大的一个.

定理6稍弱的形式是阿·维诺格拉朵夫(А.И.Виноградов)独立证明的[1]. 我们容易证明,如果(4)式成立,那末定理6是显然成立的. 因为取$B=A+1$. 将(4)代入(5)的左端即得

$$\sum_{k\leqslant x^{1/2}/(\ln x)^B} O(x^{\frac{1}{2}}\ln x)=O\left(\frac{x}{(\ln x)^{B-1}}\right)=O\left(\frac{x}{(\ln x)^A}\right).$$

公式(4)与所谓的广义黎曼猜测是等价的. 但在不少情况下,当需要用到公式(4)时,我们可以用(5)来代替. 这正是定理6的重要之处.

§18. 哥德巴赫问题

哥德巴赫(C. Goldbach)问题是1742年他写信给欧拉时提出来的. 在信中,他提出了将整数表示为素数之和的猜想. 这个猜想可以用略为修改了的语言叙述为:

(A) 每一个$\geqslant 6$的偶数都是两个奇素数之和.

(B) 每一个$\geqslant 9$的奇数都是三个奇素数之和.

例如$20=3+17$, $22=11+11$, $29=3+7+19$, $31=5+7+19$等.

显然,命题(B)是命题(A)的推论. 事实上,如果命题(A)成立. 那么对N是任何奇数$\geqslant 9$. (即$N-3$是偶数且$\geqslant 6$),由命题(A)的成立可知有奇素数q_1与q_2使

[1] А. И. Виноградов, О плотностной Гипотезе для L-рядов дирихле, ИАН СССР, сер. мат; **29**(1965), 903~934.

$$N-3=q_1+q_2,$$

所以

$$N=3+q_1+q_2.$$

因此命题(B)也成立．这说明命题(A)是最本质的．

从哥德巴赫写信起到今天，已经积累了不少关于该问题的宝贵资料．例如皮平(N. Pipping)核对过，当偶数 $n\leqslant 10^5$ 时，命题(A)是正确的．以后，申氏[1]又进一步核对了，当偶数 $n\leqslant 3.3\times 10^7$ 时，命题(A)都是对的．但是至今我们还不能确定这两个命题的真假．

1900 年，希尔伯特 (D. Hilbert) 在第二届国际数学会的著名演讲中，把黎曼猜测(见 §14)、哥德巴赫猜测(A)与孪生素数猜测(见 §19)，作为十九世纪最重要的未解决问题之一，介绍给二十世纪的数学家来解决，即所谓希尔伯特第八问题．

在1912年召开的第五届国际数学会上，朗道(E. Landau)曾经说过，既使要证明下面较弱的命题(C)，也是现代数学家所力不能及的．

(C) 存在一个正整数 c，使每一个 $\geqslant 2$ 的整数都可以表示为不超过 c 个素数之和．

注意：如果命题(A)成立，那末命题(C)显然也成立，而且 $c=3$．

1921 年，哈代(G. H. Hardy)在哥本哈根召开的数学会上说过，命题(A)的困难程度是可以和任何没有解决的数学问题相比的．

设 $r_2(N)$ 为将偶数 N 表为两个素数之和的表示法个数，

[1] Shen Mok Kong, On Checking the Goldbach Conjecture, Novdisk, Tidskr, Infor; -Behand; **4** (1964).

又设 $r_3(N)$ 为将奇数 N 表成三个素数之和的表示法个数. 例如

$$10=3+7=7+3=5+5,\ 12=5+7=7+5,$$

$$11=3+3+5=3+5+3=5+3+3,$$

所以 $r_2(10)=3$, $r_2(12)=2$, $r_3(11)=3$ 等.

哈代与李特伍德在 1922 年还进一步猜测:

(D) $r_2(N)=2\prod\limits_{\substack{p|N\\p>2}}\frac{p-1}{p-2}\prod\limits_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\frac{N}{(\ln N)^2}(1+o(1))$, 当 $2|N$.

(E) $r_3(N)=\frac{1}{2}\prod\limits_{p|N}\left(1-\frac{1}{(p-1)^2}\right)\prod\limits_{p\nmid N}\left(1+\frac{1}{(p-1)^3}\right)\frac{N^2}{(\ln N)^3}(1+o(1))$, 当 $2\nmid N$.

命题(A), (B)是哥德巴赫问题原始的算术语言提法, 而命题(D), (E)则是哥德巴赫问题的分析语言的提法. 命题(D), (E)比命题(A), (B)更加深刻. 由它们不仅能推出对于充分大的整数, 命题(A), (B)都成立, 而且给出了充分大的整数表为素数和的表示法个数的渐近公式.

近七十年来, 哥德巴赫问题吸引了世界上很多著名数学家来研究它. 取得了很好的成绩. 研究哥德巴赫问题产生的研究方法不仅对数论有广泛应用, 而且也可以用到不少其他数学分支中去.

我国著名数学家华罗庚早在三十年代就开始研究这一问题, 并得到了重要成果. 解放后, 在他的倡议与领导下, 我国青年数学工作者, 从五十年代初, 就开始研究这一问题, 他的学生们不断得到重要成果, 获得国内外的高度评价, 特别是陈景润的结果, 尤为突出.

我们将在下面介绍这个问题的一些重要结果.

首先是史尼尔曼(Л. Г. Шнирельман)在1930年(哥德巴赫提出猜想后的188年)证明了命题(C),即:

定理1(史尼尔曼). 任何$\geqslant 2$的整数都可以表示为不超过c个素数之和,这儿c是一个常数.

史尼尔曼不仅证明了命题(C),而且在他的论文中,引入了关于自然数集合很重要的概念——“密率”. 这一概念后来有了广泛发展与应用.

命s表示最小的正整数,使每一充分大的整数都可以表示成为不超过s个素数之和. 我们称s做史尼尔曼常数. 史尼尔曼的方法不仅能够得到s的存在性,而且可以得到s的明确上界. 由他的方法给出$s\leqslant 800,000$. 不少数学家改进了s的上界估计. 例如我国数学家尹文霖就在1956年证明过$s\leqslant 18$. 目前关于s的最佳估计是沃恩(R. C. Vaugham)得到的. 他证明了:

定理2(沃恩)[1][2]. 1)每一充分大的奇数是不超过5个素数之和. 2)每一充分大的偶数是不超过6个素数之和. 3)每一个$\geqslant 2$的整数都是不超过27个素数之和.

哈代与李特伍德在这一世纪的二十年代,系统地开创与发展了堆垒数论中的一个崭新的分析方法. 这个方法就是著名的“圆法”. 他们在未经证明的广义黎曼猜测成立的假定下(即假定公式(17.4)成立),证明了命题(E). 为了取消他们证明中用到的未经证明的猜测,就需要估计某种类型的“指数和”. 在三十年代,依·维诺格拉朵夫创造了一系列估计指数

---

[1] R. C. Vaugham, A note on Schirel'man's approach to Goldbach's Problem, BLMS; **8**, **3**, **24** (1976), 245~250.

[2] R. C. Vaugham, On the estimation of Schirel'man's Constant, *J für reine and ang. Math.*; **290** (1977), 94~108.

和的重要方法．从而使他在1937年证明命题(E)．当然由此推出命题(B)对于充分大的奇数都成立，即

定理3(依·维诺格拉朵夫)．设N是奇数，那末

$$r_3(N)=\frac{1}{2}\prod_{p|N}\left(1-\frac{1}{(p-1)^2}\right)\prod_{p\nmid N}\left(1+\frac{1}{(p-1)^3}\right)\frac{N^2}{(\ln N)^3}(1+o(1)).$$

由此推出，每一充分大的奇数都是三个奇素数之和．

巴雷德金(К. Г. Бороздкий)算过，当奇数$n\geqslant e^{e^{16.038}}$(这个数共4,008,600位)时，就能表示成为三个奇素数之和．换句话说，除掉适合于$n\leqslant e^{e^{16.038}}$的有限多个奇数外，命题(B)都成立．但$e^{e^{16.038}}$这个数实在太大了，无法逐一验证对小于它的奇数来说命题(B)是否成立．所以说命题(B)是基本上被证明了．

假定N是充分大的偶数，那末$N-3$是充分大的奇数．由定理3可知

$$N-3=q_1+q_2+q_3,$$

这儿q_1，q_2，q_3是奇素数，所以

$$N=3+q_1+q_2+q_3.$$

即充分大的偶数都可以表示为不超过4个素数之和．所以由定理3可以推出史尼尔曼常数$s\leqslant 4$．这是史尼尔曼方法所达不到的(史尼尔曼方法目前只能证明$s\leqslant 6$，请比较定理2)．

1938年，我国著名数学家华罗庚及一些外国数学家独立地证明了命题(A)对于几乎所有的偶数都成立．即假设$M(x)$表示不超过x，而又不能表示成为两个素数之和的偶数个数，那末

$$\lim_{x\to\infty}\frac{M(x)}{x}=0.$$

换句话说，使命题(A)成立的偶数的"出现概率"等于1. 华罗庚证明的结果比其他人的更强一些，他证明了：

定理4(华罗庚). 设k是任何一个固定的自然数. 则几乎所有的偶数都可以表成$p_1+p_2^k$，此处p_1, p_2都是素数.

另一个研究哥德巴赫问题的方法是筛法. 最原始的筛法就是埃拉多斯染尼氏筛法(见§4). 布朗(V. Brun)与赛尔贝尔格曾先后对这个方法作出过重要贡献. 用筛法来处理命题(A)时，需将命题(A)中的素数换成"殆素数". 所谓殆素数就是素因数(包括相同的与相异的)的个数不超过某一固定常数的自然数. 例如$6=2\times3$, $8=2\times2\times2$, $10=2\times5$, $12=2\times2\times3$, $21=3\times7$，所以6, 10, 21是素因数个数不超过2的殆素数. 6, 8, 10, 12, 21都是素因数个数不超过3的殆素数. 凡是素数显然都是殆素数.

为叙述简单起见，引入下面两个命题：

(F) 每一个充分大的偶数都是素因数个数分别不超过a与b的两个殆素数之和. 记为(a, b).

(G) 每一个充分大的偶数都可以表示为一个素数与一个素因数个数不超过c的殆素数之和. 记为$(1, c)$.

在命题(F)中取$a=1$，即得命题(G). 但是因为处理这两个命题所用的方法有些差异，所以我们还是分开写. 处理命题(F)用的是初等方法. 但处理命题(G)时，还需要高深分析的工具，即用到复变函数论. 哥德巴赫猜想，即命题(A)，本质上就是要证明(1, 1)成立.

首先是布朗在1920年证明了(9, 9)，即：

定理5(布朗). 每一充分大的偶数都可以表示为素因数个数都不超过9的两个殆素数之和.

关于命题(G)，首先是瑞尼(A. Renyi)在1948年证明了

(1, c)，即：

定理 6(瑞尼)．存在一个正常数 c，使每一充分大的偶数都可以表示为一个素数与一个素因数个数不超过 c 的殆素数之和．

不少数学家改进了布朗与瑞尼的结果．拉代马哈 (H. Rademacher) 在 1924 年证明了(7, 7)，埃斯特曼(T. Estermann)于 1932 年证明(6,6)．布赫夕塔布(A. A. Бухштаб)又于 1938 年及 1940 年分别证明了 (5, 5) 与 (4, 4)．笔者于 1956 年证明了(3, 4)．同年阿·维诺格拉朵夫证明了(3, 3)．1957 年，笔者又证明了(2, 3)．关于命题(G)，1962 年，潘承洞与巴尔巴恩 (M. Б. Барбан) 独立证明了 (1, 5)．1963 年，潘承洞、巴尔巴恩与笔者又都证明了(1, 4)．1965 年，阿·维诺格拉朵夫，布赫夕塔布与朋比尼都证明了(1, 3)．1966 年，我国著名数学家陈景润在对筛法作了新的重要改进之后，终于证明了(1, 2)，即：

定理 7(陈景润)[1]．每一个充分大的偶数都是一个素数与一个素因数个数不超过 2 的殆素数之和．

换句话说，命题 (F) 与 (G) 的研究已告结束．因此关于哥德巴赫问题，现在剩下需要研究的就只有命题 (A) 与 (D) 了．

埃氏筛法在近六十年来被改进后，首先是用来处理哥德巴赫问题的．但这种改进后的筛法是有广泛应用的．最直接的应用就是用于素数论．只要将困难问题中的素数换成殆素

[1] 陈景润，大偶数表为一个素数及一个不超过二个素数的乘积之和，科学通报，**17**(1966)，385～386；中国科学，**2**(1973)，111～128. 参看潘承洞，丁夏畦与王元，表大偶为一个素数及一个殆素数之和，科学通报，**8** (1975)，358～360.

数，例如将命题(A)换成命题(F)，(G)，就有可能用筛法来进行处理了.

由于最近关心哥德巴赫问题的人比较多，所以我们这里介绍得稍详细些. 有兴趣更进一步了解史尼尔曼密率方法，圆法与筛法处理哥德巴赫问题的读者，请看华罗庚著：«指数和的估计及其在数论中的应用»第一章与第五章.

§19. 孪生素数问题

1) 3, 5; 5, 7; 11, 13; 17, 19; 29, 31; …; 101, 103; …; 10, 016, 957, 10, 016, 959; …; 10^9+7, 10^9+9; …

这些素数对中二者相差都是 2. 假定 p 是素数，而 $p+2$ 也是素数，我们就称$(p, p+2)$是一对孪生素数.

很久以前，人们就问孪生素数对是否有无穷多？但是至今还不能回答这个问题.

人们积累了很多宝贵的资料说明，似乎应该有无穷多对孪生素数. 这就叫做孪生素数猜想. 例如已知小于 10^5 的自然数中，有 1,224 对孪生素数，小于 10^6 时，有 8,164 对孪生素数，而小于 3.3×10^7 时，共有 152,892 对孪生素数. 目前所知道的最大的孪生素数对是：

1,000,000,009,649, 1,000,000,009,651.

假如孪生素数对真有无穷多，那末在 §16 提出的一个问题，即寻找函数 $f_2(n)$，使当 n 充分大时有

$$d_n=p_{n+1}-p_n\geqslant f_2(n),$$

就得到了彻底的解决，即

$$f_2(n)=2.$$

设 $Z(x)$ 表示不超过 x 的自然数中，孪生素数的对数．例如 $Z(20)=4$，$Z(10^5)=1,224$，$Z(3.3\times10^7)=152,892$ 等．所谓孪生素数猜想即要证明：

$$(1)\qquad Z(x)\to\infty\,(\text{当 } x\to\infty).$$

哈代与李特伍德在 1922 年，进一步猜想关系式

$$(2)\qquad Z(x)=2\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\frac{x}{(\ln x)^2}(1+o(1))$$

应该成立．哈代与李特伍德猜想相当于孪生素数定理．公式(2)中的常数取值

$$\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)=0.6601\cdots$$

不少宝贵的数据似乎支持公式(2)是对的．

孪生素数猜想也是素数论的中心问题之一．设 a, b, c 为整数．我们还可以研究方程

$$(3)\qquad ax+by=c$$

存在素数解 x, y 或存在无穷多组素数解的问题．取 $a=1$, $b=1$, $c\geqslant6$ 为偶数即得哥德巴赫问题(见 §18，命题(A))．又取 $a=1$, $b=-1$, $c=2$ 即得孪生素数问题．

目前，从筛法的角度看，哥德巴赫问题与孪生素数问题是“姊妹问题”，往往用同一方法可以得到两个问题相类似的结果．用筛法也得到了关于孪生素数猜想一些很好的结果．例如：

定理 1(布朗)．级数 $\sum_{p^*}\frac{1}{p^*}$ 收敛，此处 p^* 经过所有的孪生素数．

如果级数 $\sum_{p^*}\frac{1}{p^*}$ 发散，那末孪生素数对数有无穷多的猜想就得到证明了．但是很遗憾，由 $\sum_{p^*}\frac{1}{p^*}$ 的收敛，并不能得

出孪生素数对数有限或无穷的结论.

定理 2(陈景润). 存在无穷多个素数 p, 使 $p+2$ 为素因数个数不超过 2 的殆素数.

2) 5, 7, 11; 11, 13, 17; 17, 19, 23; …; 101, 103, 107; …; 10, 014, 491, 10, 014, 493, 10, 014, 497; … 都是一些相差各等于 2 与 4 的素数组. 假定 p 是素数, 而 $p+2$ 与 $p+6$ 也都是素数, 我们就叫 $(p, p+2, p+6)$ 是一个**三生素数组**. 由这些数据, 似乎建议三生素数组应该有无穷多? 这就是三生素数猜想. 这比孪生素数猜想更难. 我们也可以有类似哈代与李特伍德猜想(2)的三生素数定理的猜想.

更一般些, 假定 $n>1$ 及 $l_1<\cdots<l_{n-1}$ 是 $n-1$ 个自然数. 假定 p 是素数, 且 $p+l_1, \cdots, p+l_{n-1}$ 都是素数, 我们就称

$$(p, p+l_1, \cdots, p+l_{n-1}) \tag{4}$$

是一个 **n 生素数组**.

我们有下面的猜想, 如果对于任意素数 q, n 个整数 $0, l_1, \cdots, l_{n-1}$ 模 q 互不同余的个数都小于 q, 那末 n 生素数组(4)就有无穷多. 这一猜想叫 n 生素数猜想. 我们也可以有 n 生素数定理的猜测. 取 $n=2$, $l_1=2$ 即得孪生素数猜想. 又取 $n=3$, $l_1=2$, $l_2=6$ 即得三生素数猜想, 所以 n 生素数猜想是包有孪生素数猜想与三生素数猜想作为特例的.

在平面几何中, 我们都知道, 一个三角形的任意两边之和必大于第三边, 这就是三角不等式. 在数学中有不少这类不等式. 关于 $\pi(x)$, 也有这样的猜想, 即对于自然数 $x>1$, $y>1$ 总有

$$\pi(x)+\pi(y)\geqslant\pi(x+y). \tag{5}$$

朗道曾经证明过当 $x=y$ 充分大时, 猜想(5)是对的. 近年来,

汉斯勒与黎加尔斯[1]竟借助于电子计算机证明，猜想(5)与n生素数猜想是互相矛盾的，即这两个猜想至少有一个不成立．也许猜想(5)不成立的可能性更大一些．

§20. 华林–哥德巴赫问题

比哥德巴赫问题更广，有所谓华林(E. Waring)–哥德巴赫问题．设k是一个自然数．给出自然数N，问以素数为变量的方程

$$p_1^k+\cdots+p_s^k=N \tag{1}$$

在什么条件下有解？又在什么条件下有解数的渐近公式？这个问题就叫做华林–哥德巴赫问题．

当$k=1$, $s=2$, $N\geqslant 6$为偶数及当$k=1$, $s=3$, $N\geqslant 9$为奇数，我们就分别得到关于偶数与奇数的哥德巴赫猜测(见§18，命题(A)，(B)，(D)，(E))．

我国著名数学家华罗庚系统地研究了这个问题，获得了很突出的成就．他的结果汇集在他的专著《堆垒素数论》(科学出版社，1963)之中，我们现在仅举其中的几个结果．

1）假定

$$s\geqslant\begin{cases}2^k+1, & \text{当 } 1\leqslant k\leqslant 10,\\ 2k^2(2\ln k+\ln\ln k+2.5), & \text{当 } k>10.\end{cases} \tag{2}$$

设$p^\theta \| k$(即$p^\theta | k$，而$p^{\theta+1}\nmid k$)及

$$K=\prod_{(p-1)|k}p^r,$$

[1] D. Hensley and I, Richards, On the incompartibility of two conjectures concerning primes, *Proc. Symp. Pure Math.*; **24**(1973), 123～127.

p 表示表素数及

$$\gamma=\begin{cases}\theta+2, & \text{当 } p=2, \text{ 而 } 2\mid k, \\ \theta+1, & \text{其他情形}.\end{cases}$$

在上述假定下，我们有：

定理 1（华罗庚）．每一充分大的适合于同余式

$$N\equiv s \pmod K$$

的正整数 N 都可以表示为 s 个素数的 k 次方幂之和，即方程(1)有解，而且方程(1)的解数有一个渐近公式．（在此就不具体写了）．

例 1．取 $k=1$, $s=3$．那末 $(2-1)\mid 1$, $(p-1)\nmid 1\ (p>2)$，所以 k 中只有一个素因数 2. 而且 $\theta=0$，所以 $K=2$．从而由定理 1 可知，每一充分大的奇数 N 都是三个素数之和，而且 $N=q_1+q_2+q_3$ 的素数解 (q_1, q_2, q_3) 的个数有一个渐近表达式．这就是关于哥德巴赫问题的依·维诺格拉朵夫定理（见定理 18.3）．

例 2．取 $k=2$, $s=5$．那末 K 中只有素因数 2 和 3，所以 $K=2^3\times 3=24$．从而每一充分大的模 24 同余于 5 的正整数都是 5 个素数的平方和，而且有解数的渐近公式．

例 3．取 $k=3$, $s=9$. 那末 K 中只有素因数 2，所以 $K=2$. 从而每一充分大的奇数都是 9 个素数的立方和，而且有解数的渐近公式．

2) 如果仅仅只要求方程(1)有解，而不要求有解数的渐近公式，那末对 s 的要求还可以大大降低．命 $H(k)$ 表示具有下述性质的最小整数 s: 它使每个充分大的 $\equiv s \pmod K$ 的整数都能表成 s 个素数的 k 次方幂之和．关于 $H(k)$ 的具体表达式，在这里就不写了．但 $H(k)$ 适合于 $H(k)\sim 4k\ln k$ $(k\to\infty)$．

定理 2(华罗庚). 假定 $s \geqslant H(k)$, 那末每一适合于 $N \equiv s \pmod{K}$ 的充分大的整数 N 都可以表示成 s 个素数的 k 次方幂之和.

定理 3(华罗庚). 当 $4 \leqslant k \leqslant 8$ 时有 $H(4) \leqslant 15$, $H(5) \leqslant 25$, $H(6) \leqslant 37$, $H(7) \leqslant 55$ 及 $H(8) \leqslant 75$.

给予正整数组 $N_1, \cdots, N_k$ 之后, 我们还可以进一步研究以素数 $p_1, \cdots, p_s$ 为变量的方程组

$$
\left\{\begin{array}{l}
p_1^k+\cdots+p_s^k=N_s, \\
p_1^{k-1}+\cdots+p_s^{k-1}=N_{s-1}, \\
\cdots\cdots\cdots\cdots \\
p_1+\cdots+p_s=N_1 .
\end{array}\right. \tag{3}
$$

在什么条件下, (3)有解? 在什么条件下, 有解数的渐近公式呢? 这个问题也获得了与前面一个方程相类似的圆满结果.

还可以考虑更广泛的问题. 有兴趣的读者请看华罗庚著《堆垒素数论》.

§ 21. 多项式与素数

由上面讲的一些材料, 多少可以看出, 自然数列中素数出现的规律是很复杂的. 各种形状的数, 往往既可能是素数, 又可能是复合数. 现在提出这样一个问题, 是否存在整系数多项式, 使对于每一个整数 x, $f(x)$ 都是素数? 答案是否定的.

定理 1. 如果

$$f(x)=a_n x^n+a_{n-1} x^{n-1}+\cdots+a_1 x+a_0$$

是一个整系数多项式, 其中 $a_n>0$, 那末有无穷多个整数 x, 使 $f(x)$ 为复合数.

证　因为

$$f(x)=x^n\left(a_n+\frac{a_{n-1}}{x}+\cdots+\frac{a_1}{x^{n-1}}+\frac{a_0}{x^n}\right),\quad x>0,$$

所以

$$f(x)=a_nx^n(1+o(1))\quad (当\ x\to\infty)$$

同理可知

$$f'(x)=na_nx^{n-1}(1+o(1))\quad (当\ x\to\infty).$$

因此存在自然数 x_0 充分大，当 $x\geqslant x_0$ 时有

(1) $$l=f(x_0)>1$$

及

(2) $$f(x)>f(x_0).$$

我们将证明，对于任何自然数 k，$f(x_0+kl)$ 都是复合数．由二项式展开可知

$$\begin{aligned}(x+h)^m-x^m&=\binom{m}{1}x^{m-1}h+\binom{m}{2}x^{m-2}h^2+\cdots\\&\quad+\binom{m}{m-1}xh^{m-1}+h^m\\&=h\left(\binom{m}{1}x^{m-1}+\binom{m}{2}x^{m-2}h+\cdots\right.\\&\quad\left.+\binom{m}{m-1}xh^{m-2}+h^{m-1}\right),\end{aligned}$$

因此

$$h\mid((x+h)^m-x^m),\quad m=1,\ 2,\ \cdots.$$

由于

$$\begin{aligned}f(x+h)-f(x)&=a_n((x+h)^n-x^n)\\&\quad+\cdots+a_1((x+h)-x),\end{aligned}$$

所以

$$h \mid (f(x+h)-f(x)).$$

即得

$$kl \mid (f(x_0+kl)-f(x_0)).$$

于是由(1)可得

$$f(x_0+kl)-l=tkl \quad (t\text{是整数}),$$

$$f(x_0+kl)=(tk+1)l.$$

由(1),(2)可知$f(x_0+kl)>f(x_0)=l>1$,所以$f(x_0+kl)$有真因数l,因此它是一个复合数．定理证完．

既然不存在一个整系数多项式$f(x)$，使当$x=1, 2, \cdots$时,$f(x)$都取素数．那末是否存在整系数多项式$F(x)$,使当$x=1, 2, \cdots$时,$F(x)$取无穷多个素数呢？

例 1．假定$F(x)=x$,答案是肯定的，即素数有无穷多(定理3.1)．

例 2．假定$F(x)=kx+l$,其中$(k, l)=1$．答案也是肯定的．这就是狄里赫勒定理(定理17.1)．

但是我们还不知道任何一个次数大于1的多项式$F(x)$,使当$x=1, 2, \cdots$时，$F(x)$取无穷多个素数．

最简单的多项式是$F(x)=x^2+1$．当$x=1, 2, 4, 6, 10$时,x^2+1分别等于2, 5, 17, 37, 101都是素数．更多的数据表明,当$x\leqslant 10^4$时,有842个x使x^2+1取素数．当$x\leqslant 10^5$时,有6,656个x使x^2+1取素数．而当$x\leqslant 1.8\times 10^5$时，有11,223个$x$使$x^2+1$取素数．看来应该有无穷多个自然数$x$使$x^2+1$取素数．但是我们还不能给以证明．

其次,有没有无穷多个自然数x使x^3+2取素数呢？我们也不能回答．但已知$3=1^3+2$, $29=3^3+2$, $127=5^3+2$, $24,391=29^3+2$都是素数．

孔恩(P. Kuhn)与笔者分别对多项式x^2+1与x^3+2得

到了下面的结果:

定理 2. 1)存在无穷多个自然数 x, 使 x^2+1 为素因数个数不超过 3 的殆素数. 2)存在无穷多个自然数 x, 使 x^3+2 为素因数个数不超过 4 的殆素数.

更一般些,还有

定理 3(布赫夕塔布, 黎切尔特)[1][2]. 假定 $F(x)$ 是一个首项系数是正的既约整系数多项式(所谓既约, 即 $F(x)$ 不能分解成两个次数 $\geqslant 1$ 的整系数多项式的乘积). 记同余式

$$F(x)\equiv o(\bmod p),\ 1\leqslant x\leqslant p$$

的解数是 $\rho(p)$. 假定对于任何素数 p 都有 $\rho(p)<p$. 如果 $F(x)$ 的次数是 k, 那末存在无穷多个自然数 x, 使 $F(x)$ 为素因数个数不超过 $k+1$ 的殆素数.

有进一步的猜想, 即对于任何适合于定理 3 条件的多项式 $F(x)$, 都存在无穷多个自然数 x, 使 $F(x)$ 取素数.

更一般些, 还有辛哲尔(A. Schinzel)猜测: 假定有 n 个整系数多项式 $F_1(x)$, …, $F_n(x)$, 它们的首项系数都是正的, 而且都是既约的. 假定同余式

$$F_1(x)\cdots F_n(x)\equiv o(\bmod p),\ 1\leqslant x\leqslant p$$

的解数为 $\rho(p)$. 如果对于任意素数 p 都有 $\rho(p)<p$, 那末存在无穷多个自然数 x 使 $F_1(x)$, …, $F_n(x)$ 同时都取素数. 并且有类似的"素数定理"的猜测.

例 1. 取 $F_1(x)=x$, $F_2(x)=x+2$, 就得到孪生素数猜测.

---

[1] А. А. Бухштаб, Комбирнаторное Усиление Метода Эратосфенова Решета, *УМН СССР*, **22** (1967), 199~226.

[2] H. E. Richert, Selberg's sieve with weights, *Mathematika*; **16** (1969), 1~22.

例 2. 取 $F_1(x)=x$, $F_2(x)=x+2$, $F_3(x)=x+6$, 就得到三生素数猜测.

例 3. 取 $F_1(x)=x$, $F_2(x)=x+l_1$, $\cdots$, $F_n(x)=x+l_{n-1}$, 此处 $l_1<\cdots<l_{n-1}$ 为自然数. 假定对于任何素数 p, 诸整数 $0, l_1, \cdots, l_{n-1}$ 模 p 互不同余的个数皆小于 p, 即得 n 生素数猜测(见 §19).

已知多项式

$$x^2-x+17,$$

当 $x=1, \cdots, 16$ 时, 都取素数. 又已知多项式

$$x^2-x+41,$$

当 $x=1, \cdots, 40$ 时, 都取素数. 现在提一个问题: 任意给予一个自然数 N, 能不能找到素数 p, 使当 $x=1, \cdots, N$ 时, 多项式

$$x^2-x+p$$

都取素数?

这个问题比孪生素数猜测与三生素数猜测更难. 假定上面的问题得到了正面的答案. 取 $q_1\geqslant 3$ 为素数, 那末存在素数 q_2 使当 $x=1, \cdots, q_1$ 时,

$$x^2-x+q_2$$

都取素数. 显然 $q_2>q_1$ (否则若 $q_2\leqslant q_1$, 则当 $x=q_2$ 时, 即得复合数 q_2^2). 又对于素数 q_2, 存在素数 q_3 使当 $x=1, \cdots, q_2$ 时,

$$x^2-x+q_3$$

都取素数. 依次类推, 存在素数数列 $q_1<q_2<\cdots$, 使当 $x=1, \cdots, q_{i-1}$ 时,

$$x^2-x+q_i$$

都取素数. 特别取 $x=1, 2$, 即得无穷多对孪生素数 $(q_i, q_i+$

2) $(i=2, 3, \cdots)$. 又取 $x=1, 2, 3$, 即得无穷多组三生素 (q_i, q_i+2, q_i+6) $(i=2, 3, \cdots)$. 从而孪生素数猜测与三生素数猜测将都有了肯定的答复.

从这里也可以看出,数论中能够建议的猜想,常常比能解决的要多得多了.

§ 22. 表整数为素数与整数平方之和的问题

哈代与李特伍德在 1922 年曾猜测,每一个充分大的不是完全平方的自然数都可以表示为一个素数与一个自然数的平方之和. 这一猜测至今仍没有解决.

假定 p 是奇素数, 那末 $\frac{p-1}{2}$ 与 $\frac{p+1}{2}$ 都是自然数, 所以

$$\left(\frac{p+1}{2}\right)^2=\left(\frac{p-1}{2}\right)^2+p.$$

另一方面, 如果 $n=3k+2$, 其中 k 是自然数. 现在来证明不存在自然数 x 与素数 q 使

$$n^2=x^2+q.$$

假如上式成立,那末

$$q=n^2-x^2=(n+x)(n-x).$$

因为 q 是素数,所以 $n+x=q$, $n-x=1$, 从而

$$q=2n-1=6k+4-1=3(2k+1).$$

这是不可能的.

因此我们证明了存在无穷多个自然数的完全平方, 它们

都可以表示成为一个素数与一个自然数的平方之和. 另一方面,也存在无穷多个自然数的完全平方,它们都不能表示成一个素数与一个自然数的平方之和.

哈代与李特伍德在1922年还猜测,每一充分大的整数都可以表示为一个素数与两个整数的平方之和. 这个猜测是林尼克在1960年解决的.

定理1(林尼克)[1]. 每一充分大的整数 n 都可以表示成一个素数与两个整数的平方之和.

在定理1中,我们也可以得到将整数 n 表示成一个素数与两个整数的平方之和的表法个数的渐近公式. 用类似的方法还可以证明:

定理2. 对于任意整数 a, 皆存在无穷多个素数 p 表示成为

$$p=x^2+y^2+a,$$

其中 x 与 y 都是整数.

注意: 多项式 x^2+y^2+a 是两个变数 x, y 的多项式.

§23. 模 p 的剩余类分布问题

假定 $k>1$ 为整数及 p 表示素数. 在§11中,我们已经定义了模 p 的 k 次剩余与 k 次非剩余.

我们用 $n_k(p)$ 表示模 p 的最小正 k 次非剩余. 例如 $n_2(7)=3$, $n_2(11)=2$ 等. 最有名的问题是估计 $n_2(p)$ 的上界. 目前关于 $n_2(p)$ 的最佳估计是布尔吉斯于1957年证明的.

---

[1] Ю. В. Линник, Дисперсионный мегод в бинарных аддитивных Задачах, изд. Лин. ун-та; 1961.

定理 1(布尔吉斯)[1]. $n_2(p)=O(p^{\frac{1}{4\sqrt{e}}+\varepsilon})$, 其中 ε 是任意给定的正数,而与"O"有关的常数仅依赖于 ε.

关于 $n_k(p)$, 笔者以后也证明了类似的结果:

定理 2. 假定 ε 为任意正数,则当 p 充分大时有:

1) $n_k(p)\leqslant p^{\frac{1}{4e^{\frac{k-1}{k}}}+\varepsilon}\quad(k\geqslant 2)$,

2) $n_k(p)\leqslant p^{\frac{1}{12}}\quad(n\geqslant 21)$,

3) $n_k(p)\leqslant p^{\frac{\ln\ln k+3}{4\ln k}}\quad(k\geqslant e^{33})$.

但这些结果与理想的猜想结果还相距很远. 一些数据表明似乎应该有:

$$n_2(p)=O((\ln p)^2) \tag{1}$$

或者甚至可能有:

$$n_2(p)=O((\ln p)^{1+\varepsilon}), \tag{2}$$

此处与"O"有关的常数仅依赖于 ε. 但是可以证明

$$n_2(p)=\Omega(\ln p). \tag{3}$$

在广义黎曼猜测真实的假定下(即假定(17.4)成立), 可以证明(1)式成立.

关于 $n_k(p)\,(k>2)$ 的猜测结果也是与 $n_2(p)$ 完全一样的.

另一个有名的问题是关于模 p 的最小原根问题. 假定 g 是一个自然数,且 $p\nmid g$, 那末由定理 8.1 可知:

$$g^{p-1}\equiv 1(\bmod p).$$

如果当 $1\leqslant l<p-1$ 时都有

$$g^l\not\equiv 1(\bmod p),$$

我们就称 g 是模 p 的原根. 可以证明模 p 的原根是存在的

---

[1] D. A. Burgess, The distribution of guadratic residues and non-residues, *Mathematika*; **4**(1957), 106~112.

(见华罗庚著《数论导引》第三章). 我们用 $g(p)$ 来表示模 p 的最小正原根. 例如 $g(11)=2$, $g(41)=6$, $g(409)=21$, $g(467)=2$ 等. 关于原根最著名的问题之一是估计 $g(p)$ 的上界. 目前最好的结果是用布尔吉斯方法, 由布尔吉斯与笔者独立地证明的, 即:

定理 3. $g(p)=O(p^{\frac{1}{4}+\varepsilon})$, 其中 ε 为任意正数, 而与"O"有关的常数仅与 ε 有关.

同样, 这个结果与关于 $g(p)$ 的猜测结果

(3) $$g(p)=O((\ln p)^2) \text{或} g(p)=O((\ln p)^{1+\varepsilon})$$

相比, 是差得很远的.

在广义黎曼猜测真实的假定下, 可以证明:

(4) $$g(p)=O(m^6(\ln p)^2),$$

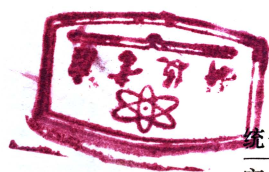
此处 m 表示 $p-1$ 的互异的素因数个数.

关于原根另一个重要问题是阿丁 (E. Artin) 在 1927 年提出的猜测, 即对于任意不等于 1, $p-1$ 及完全平方的正整数 a, 必定存在无穷多个素数 p, 以 a 为原根. 特别是存在无穷多个素数 p, 以 2 为原根.

关于这个问题, 还没有答案. 1967 年, 霍勒[1]在某种黎曼猜测成立的假定之下, 证明了阿丁猜测, 并得到了以 a 为原根的适合于 $p\leqslant x$ 的素数个数的渐近表达式.

---

[1] C. Hooley, On Artin's Conjecture, *J. reine angew. Math.*; **225** (1967), 209~220.



统一书号：7150·1947

定　　价：0.20 元